UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

Ingeniero de Sistemas

TEMA:

PROPUESTA DE UN PLAN DE CONTINGENCIA PARA SALVAGUARDAR LOS ACTIVOS DE INFORMACIÓN EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA EMPRESA PÚBLICA MUNICIPAL DE RESIDUOS SÓLIDOS RUMIÑAHUI-ASEO EPM EMPLEANDO LA METODOLOGÍA MAGERIT

AUTORES:

FABIAN PAÚL PAZMIÑO SANCHEZ

NELSON ISMAEL ALDAZ CALISPA

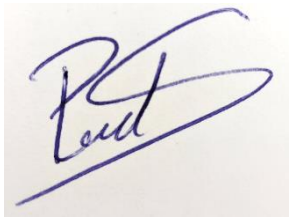
TUTOR

JOSÉ LUIS AGUAYO MORALES

Quito, marzo del 2021

CESIÓN DE DERECHOS DE AUTOR

Nosotros NELSON ISMAEL ALDAZ CALISPA, con documento de identificación N° 1714632542 y, FABIAN PAÚL PAZMIÑO SANCHEZ, con documento de identificación N° 1718211731, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: PROPUESTA DE UN PLAN DE CONTINGENCIA PARA SALVAGUARDAR LOS ACTIVOS DE INFORMACIÓN EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA EMPRESA PÚBLICA MUNICIPAL DE RESIDUOS SÓLIDOS RUMIÑAHUI-ASEO EPM EMPLEANDO LA METODOLOGÍA MAGERIT, mismo que ha sido desarrollado para optar por el título de INGENIERO DE SISTEMAS, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribimos este documento en el momento que hacemos entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.



Fabian Paúl Pazmiño Sanchez
CI:1718211731

Nelson Ismael Aldaz Calispa
CI: 1714632542

Quito, marzo del 2021

DECLARATORIA DE COAUTORIA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico titulado PROPUESTA DE UN PLAN DE CONTINGENCIA PARA SALVAGUARDAR LOS ACTIVOS DE INFORMACIÓN EN EL DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN DE LA EMPRESA PÚBLICA MUNICIPAL DE RESIDUOS SÓLIDOS RUMIÑAHUI-ASEO EPM EMPLEANDO LA METODOLOGÍA MAGERIT realizado por Nelson Ismael Aldaz Calispa y Fabian Paúl Pazmiño Sanchez, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerado como trabajo final de titulación.

Quito, marzo del 2021

Carta de Autorización

Rumiñahui
GOBIERNO MUNICIPAL
EMPRESA PÚBLICA MUNICIPAL DE RESIDUOS SÓLIDOS RUMIÑAHUI-ASEO, EPM

Oficio Nro. EPMR-GG-2020-0036-GD-O

Sangolquí, 19 de octubre de 2020

Asunto: oficio de aceptación

Señora Magíster
Patsy Malena Prieto Vélez
Directora de la Carrera de Ingeniería en Sistemas
UNIVERSIDAD POLITÉCNICA SALESIANA
Presente.

En atención al oficio S/N de 16 de octubre de 2020, suscrito por el señor Ismael Aldaz Calispa con C.I. 1714632542, mediante el cual solicita apoyo para la realización del trabajo de tesis previo a la obtención del título de Ingeniero en Sistemas con el siguiente tema:

"Propuesta de un plan de contingencia para salvaguardar los activos de información en el Departamento de Tecnología de la Información y Comunicación de la Empresa Pública Municipal de Residuos Sólidos Rumiñahui Aseo EPM empleando la metodología MAGERIT"

Al respecto, me permito informarle que el requerimiento ha sido Aceptado, la empresa se compromete en la entrega de la información, la cual deberá ser manejada con estricta confidencialidad para la ejecución de tesis por parte de los señores:

Nelson Ismael Aldaz Calispa con C.C. 17463254-2
Fabián Paúl Pazmiño Sánchez con C.C. 171821173-1

Atentamente,

Documento Firmado electrónicamente por LUIS SANTIAGO MARCILLO GOMEZ

Ing. Luis Santiago Marcillo Gomez
GERENTE GENERAL

Referencias:
- EPMR-GG-2020-0056-GD-E

NUT: EPMR-2020-0565

Acción	Siglas Unidad	Fecha	Sumilla
Elaborado por: Janeth Yadira Carvajal Morejon	GG	2020-10-19	

Dedicatoria

El presente trabajo de titulación se lo dedico en primer lugar a Dios que en el transcurso de mi vida me ha brindado la oportunidad de cumplir con mis metas trazadas, guiándome día a día para cumplir mis objetivos.

A toda mi familia sin excepción en especial a mi madre, quien ha sido mi sostén durante todo el periodo de mi educación, mención especial a mi abuelita Laura que desde el cielo me ha cuidado y ayudado espiritualmente para cumplir esta meta.

A la empresa donde laboro, mis compañeros de trabajo que con su ayuda han permitido el desarrollo de mi trabajo de titulación.

A todas mis amistades, en especial aquellas que han sabido estar en las buenas y malas, compartiendo sus experiencias y consejos para forjar mi camino trazado, aquellas amistades que no me han abandonado y continúan siendo un pilar fundamental en el desarrollo de mi vida.

Nelson Ismael Aldaz Calispa.

Este trabajo se lo dedico principalmente a mi familia que ha sido mi sostén y mi fuerza durante todos estos años de carrera especialmente a mis padres quienes me han apoyado en todas las decisiones que he tomado y me han ayudado a cumplir todas mis metas, gracias a todo su esfuerzo, amor y cariño que me han brindado.

Agradezco la oportunidad brindada por la empresa para poder realizar mi trabajo de titulación junto con mi compañero.

De igual manera a la Universidad Politécnica Salesiana, a los profesores, a mis compañeros y a todos los amigos que me han acompañado en este proceso con los que compartí grandes experiencias que las guardaré para toda la vida muchas gracias a todos.

Fabian Paúl Pazmiño Sanchez

Índice General

Índice de Tablas

Índice de Figuras

Índice de Anexos

Resumen

Las empresas pueden verse afectadas por amenazas que provoquen pérdidas y daños a los activos de información, perjudicando directamente la continuidad del negocio por lo que la empresa pública municipal de residuos sólidos Rumiñahui Aseo requirió un análisis de sus riesgos de información.

Este proyecto utilizó la Metodología MAGERIT de Análisis y Gestión de Riesgos que identificó los activos más importantes del departamento de tecnología, así como los riesgos y amenazas a los que pueden estar expuestos, para recomendar la implementación de salvaguardas.

Con la ayuda de la herramienta PILAR, que fue utilizada principalmente por MAGERIT, se identificaron los activos para realizar el análisis de riesgo, se listaron los activos críticos, así como sus amenazas y salvaguardas, se realizó una evaluación de estos para identificar los riesgo e impacto que pueden causar si se materializan las amenazas.

Finalmente, se evidenciaron los activos críticos, se elaboró un plan de seguridad que contiene un plan de ejecución y una política de seguridad. Se evidenció que, de veinte activos críticos, el 90% redujo al mínimo el impacto y los restantes bajaron su nivel de riesgo.

ABSTRACT

Companies may be affected by threats that cause loss and damage to information assets, directly undermining business continuity for which the “Empresa Pública Municipal de Residuos Sólidos Rumiñahui Aseo” required an analysis of their information risks.

This project was using the MAGERIT Methodology for Risk Analysis and Management that identified the most important assets of the technology department, as well as risks and threats to which they may be exposed, to recommend the implementation of safeguards.

With the help of the PILAR tool, which was mainly used by MAGERIT, the assets were identified to carry out the risk analysis, the critical assets were listed, as well as their threats and safeguards, an assessment of these was carried out to identify the risk and impact that they can cause if threats materialize.

Finally, the critical assets were evidenced, a security plan was elaborated containing an execution plan and a security policy. That was evidenced that out of twenty critical assets, 90% reduced to minimum´s impact and the remaining ones lowered their risk level.

INTRODUCCIÓN

Este proyecto tiene como fin en el desarrollo de una propuesta de un plan de contingencia para salvaguardar los activos de información del departamento de TIC´s empleando la metodología MAGERIT, con la ayuda de la herramienta PILAR, que permitirá que el área de tecnología tenga un conocimiento de los riesgos que puedan presentar sus activos y el tratamiento que se les pueda brindar a los más críticos.

Se ha considerado que el presente trabajo de titulación sea divido en 4 capítulos, mismos que detallan a continuación:

Capítulo 1 denominado Descripción del Objeto de Estudio, se tratará de una descripción general de la empresa que se considera como objeto de estudio, su misión y visión al año 2020, así como los servicios y las actividades que realiza la empresa.

Capítulo 2 denominado Marco Teórico, menciona el soporte contextual empleado e investigado para ser la base de los conceptos utilizados en el planteamiento del problema de estudio.

Capítulo 3 denominado Análisis de riesgos, se considera el soporte del proyecto, en donde como primer punto se define la identificación de los activos de información del departamento de tecnología, posteriormente se identifican las amenazas que puedan tener los mencionados activos, se realiza la validación de las posibles salvaguardas existentes, de igual manera se realiza un análisis de las vulnerabilidades y se determina los riesgos a los que pueden ser susceptibles los activos de información.

Capítulo 4 denominado Gestión de Riesgos, se identifican los riesgos más críticos y se toman las medidas necesarias que permitan prevenir o mitigar los riesgos encontrados, se implementan

nuevas salvaguardas y se refuerzan las ya existentes, proponiendo un plan de seguridad con el objetivo de controlar los riesgos que han sido identificados en el departamento de tecnología.

Como punto final el apartado de Conclusiones y Recomendaciones, en donde se resumen los resultados obtenidos y se realizan sugerencias para tomar a consideración por parte del departamento de tecnología.

1. ANTECEDENTES

La empresa Pública Municipal de Residuos Sólidos Rumiñahui-Aseo de aquí en adelante nombrada por sus siglas como EPMR, es una organización que contribuye a la limpieza del cantón Rumiñahui mediante la recolección de residuos sólidos generados en el cantón.

El departamento de tecnología de la institución puede desconocer el riesgo que puedan tener sus activos y verse comprometidos con la continuidad de los servicios en caso de la materialización de alguno de ellos, afectando también a la reputación de la empresa.

El proyecto de tesis radica en realizar una Propuesta de un plan de contingencia para salvaguardar los activos de información en el Departamento de Tecnología de la Información y Comunicación de la EPMR empleando la metodología MAGERIT, mismo que ayudará al departamento de tecnología y por ende a la institución a comprender los riesgos que pueden presentarse en sus activos de información, la importancia y criticidad que se debe brindar a aquellos activos que requieran mayor control, ayudando a una mejor toma de decisiones eficaz y a tiempo.

2. PROBLEMA DE ESTUDIO

El Departamento de TIC´s en la EPMR, se conforma de dos personas (Un Jefe de TICS y un Técnico en Informática), que están a cargo de las actividades tecnológicas y administrativas que han sido designadas por la máxima autoridad, considerando entre sus funciones la administración de redes, soporte al usuario, administración de usuarios, dar seguimiento a los procesos necesarios para continuar con el correcto funcionamiento de las actividades en la empresa.

Se considera que cualquier sistema de información o arquitectura tecnológica está expuesta a riesgos, esto implica que tanto software como hardware son susceptibles de diversos fallos que pueden ser provocados por errores humanos, errores físicos o incluso hasta desastres naturales, en caso de presentarse cualquier anomalía los funcionarios del departamento de tecnología deben estar en la capacidad de determinar la gravedad del problema y en la obligación de plantear una solución inmediata ante el evento suscitado.

Uno de los inconvenientes presentados, es que el departamento de tecnología no posee documentación que permita indicar las acciones a tomar en casos de amenazas o en su defecto un plan de contingencia que permita mitigar los problemas que puedan presentarse al verse expuesto a riesgos, amenazas y vulnerabilidades que impliquen perdida de información, así mismo en los equipos informáticos que la empresa posee, al verse estos afectados causarán alto impacto en el funcionamiento correcto de las actividades de la empresa.

La empresa consta con un servidor de respaldos que permite realizar un backup de los equipos de cómputo y servidores, pero existe gran riesgo en pérdida de información al no contar un sistema de bloqueo de puertos para dispositivos USB, ya que muchas veces los funcionarios realizan sus trabajos directamente en las Flash Memory o discos duros, lo que provoca que no se almacene la información en los computadores de la empresa.

Es necesario la implementación de un plan de contingencia que permita seguir lineamientos para la toma de decisiones ante la ocurrencia de un evento que puede ser perjudicial para el correcto funcionamiento de la empresa.

3. JUSTIFICACIÓN

En la actualidad la utilización de las tecnologías de la información es creciente en organizaciones y empresas, de igual manera se exponen a riesgos que puedan causar pérdida de los activos de información más críticos manejados por el departamento de tecnología.

La EPMR para su continuo funcionamiento apunta a su infraestructura tecnológica para brindar un servicio ágil a la comunidad rumiñahuense, por lo tanto, la necesidad de proteger los activos de información se convierte en objetivo primario ante la posible destrucción, pérdida, robo u otras amenazas que pueda presentar la empresa y que afecten directamente a la disponibilidad de la información, para ello se debe establecer un plan de contingencia que permita mitigar estas actividades.

Plantear la implementación de un plan de contingencia para los activos de información en el Departamento de Tecnología de la EPMR basado en la metodología MAGERIT, permitirá obtener respuestas a riesgos que puedan afectar al área, permitiendo tener una ágil toma de decisiones ante los eventos que puedan ocurrir, garantizar la seguridad, disponibilidad, integridad y confiabilidad de la información que posee el departamento y por ende la empresa.

Por lo citado anteriormente, conviene desarrollar un plan de contingencia, mismo que indicará a los funcionarios del departamento de tecnología cómo actuar y qué acciones tomar ante un posible incidente que afecte a los componentes físicos, lógicos y sobre todo precautelar la integridad de la información.

4. OBJETIVOS

El beneficiario directo del presente trabajo de tesis son por una parte la Empresa Pública Municipal de Residuos Sólidos y el Departamento de Tecnología, sus equipos informáticos, la información que debe estar bajo los criterios de confidencialidad, integridad y disponibilidad.

4.1. *Objetivo General*

Determinar un plan de contingencia para el Departamento de Tecnología de la Información y Comunicación en la Empresa Pública Municipal de Residuos Sólidos Rumiñahui-Aseo EPM, con el fin de salvaguardar sus activos de información.

4.2. *Objetivos Específicos*

- Reconocer los activos de información críticos que maneja el Departamento de Tecnología de la Información y Comunicación.
- Realizar un análisis de riesgos en el Departamento de Tecnología identificando los posibles riesgos y vulnerabilidades que pueden afectar al normal funcionamiento de los servicios que brinda.
- Delimitar las acciones a tomar para resguardar los equipos de información y la información más relevante existente.
- Proponer un plan de contingencia que mitigue los riesgos más críticos que afecten al departamento de tecnología.

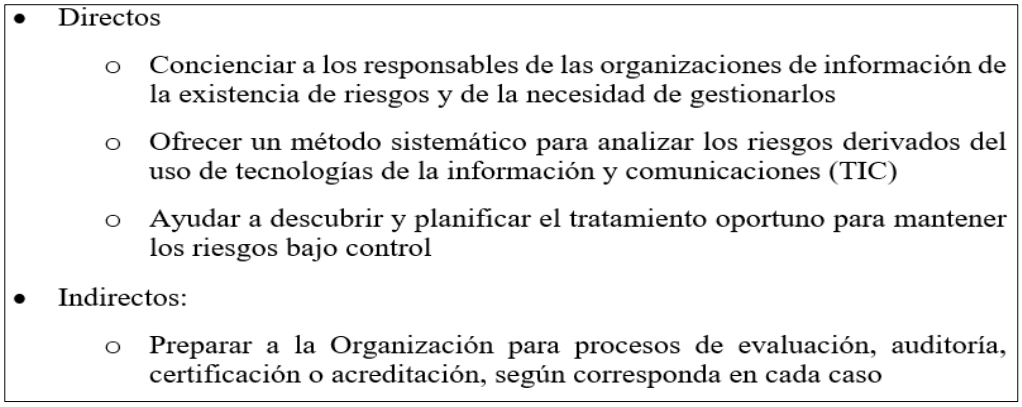
5. METODOLOGÍA

La metodología utilizada en este proyecto es la del análisis y gestión de riegos MAGERIT elaborada por la CSAE (Consejo Superior de Administración de España) dirigido a organizaciones que dependen de las tecnologías de la información para su correcto funcionamiento.

Para aplicar la metodología Magerit es necesario seguir con una serie de tareas que son, primero un análisis de riesgos para determinar el estado actual de la organización, la gestión de riesgos para revisar que hacer con estos riesgos y finalmente la realización de un plan de seguridad.

De acuerdo a (Consejo Superior de Administración Electrónica, 2012a) Magerit persigue los siguientes objetivos:

Figura 1
Objetivos de Magerit



Nota. *Objetivos Directos e Indirectos de MAGERIT Fuente: (Consejo Superior de Administración Electrónica, 2012a)*

Magerit ayuda a plantear medidas preventivas en contra de posibles ataques que vulneren la seguridad de la información, en base a un análisis de riesgos que se adapta según las necesidades de la organización que hace uso de esta metodología.

MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.(Gutiérrez, 2020).

CAPÍTULO 1

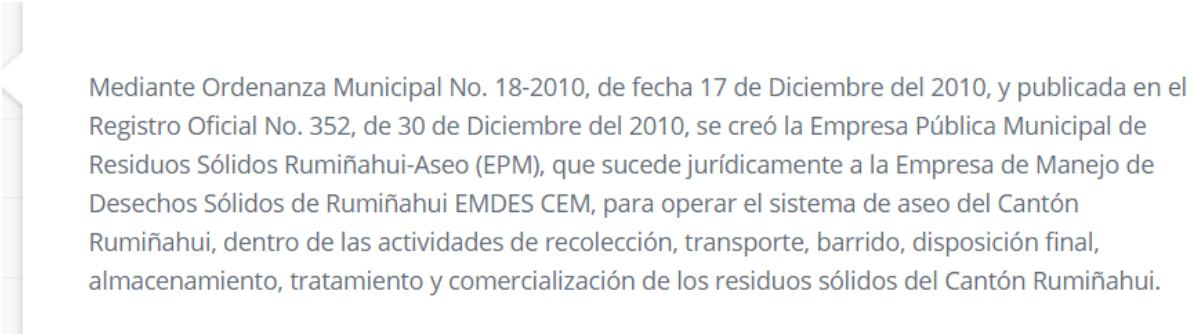
1. Descripción del Objeto de Estudio

En el presente capítulo se presentará una breve descripción de la EPMR, así como de sus actividades fundamentales para contribuir con la limpieza del cantón Rumiñahui.

1.1. *Antecedentes de la empresa*

RESEÑA HISTÓRICA

Figura 2
Historia de Creación



Nota. Reseña Histórica de la EPMR. Fuente: (*RUMIÑAHUI – ASEO, EPM*, n.d.)

En la actualidad la Empresa Pública Municipal de Residuos Sólidos Rumiñahui Aseo, cuenta con 7 Gerencias distribuidas de la siguiente manera:

- Gerencia General.
- Asesoría Jurídica.
- Gerencia Administrativa y de Talento Humano.
- Gerencia Financiera.
- Gerencia de Planificación y Gestión Empresarial.
- Gerencia Radio ECOS de Rumiñahui.
- Gerencia de Operaciones.

1.1.1. Reconocimiento de la Empresa

La EPMR tiene como meta ser reconocida a nivel nacional como la mejor empresa de recolección de residuos sólidos, para ello se plantea los siguientes propósitos:

1.1.1.1. Misión Institucional

La misión al año 2021 de la EPMR es la siguiente:

Figura 3
Misión Institucional

"Somos una Empresa Pública enfocada en la gestión integral de residuos sólidos no peligrosos y desechos sanitarios, para conservar limpio al cantón Rumiñahui."

RADIO: «Somos una radio Pública Municipal, que informa, educa y entretiene a la comunidad.»

Nota. *Misión Institucional de la EPMR. Fuente:* (*RUMIÑAHUI – ASEO, EPM*, n.d.)

1.1.1.2. Visión Institucional

Para el año 2021 la visión de la EPMR es la siguiente:

Figura 4
Visión Institucional

"Ser reconocidos a nivel nacional por nuestro modelo de gestión basado en la efectividad del servicio, tecnología e infraestructura innovadora, talento humano motivado y el compromiso ciudadano. Contribuiremos de manera decidida con el medio ambiente y el orgullo rumiñahuense."

RADIO: «Consolidarnos como el medio de comunicación de mayor credibilidad y sintonía en el cantón Rumiñahui y el valle de los chillos.»

Nota. *Misión Institucional de la EPMR. Fuente:* (*RUMIÑAHUI – ASEO, EPM*, n.d.)

1.1.1.3. Objetivos Estratégicos

Objetivo General de la Empresa:

"Mantener el cantón siempre limpio".

Objetivos Específicos de la Empresa:

- Garantizar servicios oportunos, continuos y completos cumpliendo las normativas vigentes,
- Asegurar el financiamiento y las inversiones en tecnología y el desarrollo de nuestro talento humano.
- Lograr la generación «responsable» de desechos sólidos educando de manera permanente.
- Lograr el apoyo de socios estratégicos.
- Consolidar nuestra Cultura Organizacional hacia la excelencia y efectividad de nuestros servicios.

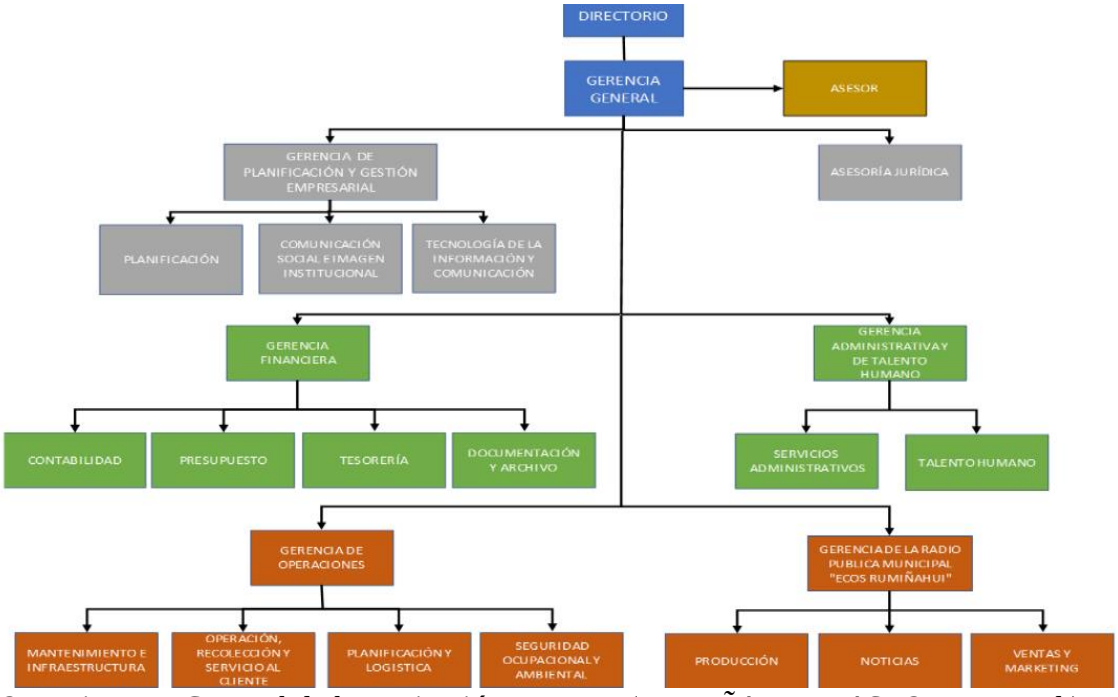
1.2. *Organigrama de la Institución*

La Empresa Rumiñahui Aseo está representada por el Directorio que es el órgano de legislación y fiscalización, y él o la Gerente(a) General que es la máxima autoridad ejecutiva de la institución. Además, cuenta con Gerentes designados con puestos de libre designación y remoción:

- Asesor Jurídico.
- Gerente de Planificación y Gestión Empresarial.
- Gerente Financiero.
- Gerente Administrativo y de Talento Humano.
- Gerente Radio Pública Municipal "Ecos de Rumiñahui".
- Gerente de Operaciones.

De la Estructura Orgánica por Procesos La Empresa Pública Municipal de Residuos Sólidos "Rumiñahui-Aseo", para el cumplimiento de su misión, objetivos y responsabilidades, desarrolla procesos internos y está conformada por:

Figura 5
Organigrama de la Organización



Nota. *Organigrama General de la Institución. Fuente: (RUMIÑAHUI – ASEO, EPM, n.d.)*

1.3. *Actividades*

La Empresa Pública Municipal de Residuos Sólidos Rumiñahui-Aseo (EPMR), ofrece los servicios que se detallan en la imagen:

Figura 6
Lista de los servicios de Aseo

Nota. *Servicios de Aseo proporcionado por la EPMR. Fuente:(RUMIÑAHUI – ASEO, EPM, n.d.)*

Los servicios ofrecidos se enlistan a continuación:

1. Recolección contenerizada.
2. Recolección Tradicional.
3. Barrido manual de calles.
4. Barrido mecánico de calles.
5. Limpieza y recolección en eventos y espectáculos públicos.
6. Recolección de desechos hospitalarios.
7. Recolección en industrias, mercados y centros comerciales.
8. Hidrolavado y limpieza de calles y plazas.
9. Recolección diferenciada de residuos sólidos.
10. Recolección de papeleras

1.4. *Recursos*

1.4.1. Personal

La institución brinda un servicio las 24 horas del día los 365 días el año, para ello se en la Tabla 1. el número de personal por área con el que cuenta la empresa:

Tabla 1.
Personal de la empresa

TIPO CARGO	NÚMERO
CHOFERES	8
OPERATIVOS	14
AYUDANTES	2
AUXILIARES	2
SUPERVISOR DE RUTA	1
RECOLECCION/BARRIDO	35
DIRECTIVOS	6
ADMINISTRATIVOS	49
TOTAL, EMPLEADOS Y TRABAJADORES	117

Nota. *La tabla muestra la cantidad de empleados que trabajan en cada área de la empresa*

Fuente: Talento Humano EPMR

1.4.2. Recursos Materiales

La EPMR, cuenta con los siguientes recursos materiales:

- Terreno.
- Maquinaria y Equipos.
- Equipos de Cómputo.
- Equipos de Oficina.
- Vehículos.
- Equipos de comunicación.
- Edificio.

1.4.3. Departamento de Tecnología De La Información y Comunicación

El área de tecnología de la EPMR pertenece a la Gerencia de Planificación y Gestión Empresarial, y es la encargada de proporcionar los servicios tecnológicos en la empresa de una manera oportuna y eficaz.

1.4.3.1. Recurso Humano Tecnológico

El personal con el que actualmente cuenta el departamento de tecnología se describe a continuación en la Tabla 2.

Tabla 2.
Personal de TICS

Nombre	Cargo	Profesión
Sr. Ing. Luis Villalta	JEFE DE TIC´s	Ingeniero De Sistemas
Sr. Ismael Aldaz	TÉCNICO EN INFORMÁTICA	Egresado de la Carrera Ingeniería en Sistemas

Nota: Lista del personal de TICS de la EPMR. Elaborado por los Autores

CAPÍTULO 2

2. Marco Teórico

2.1. *Seguridad Informática y de la Información*

La seguridad informática y de la información en las empresas se la considera un pilar importante en la era digital actual donde se mueven grandes cantidades de información y en donde mucha de esta puede estar expuesta a ataques y amenazas tanto internas como externas, por esta razón es importante mantener los activos de las empresas bien protegidos y elaborar planes de contingencia en caso de que estos ocurran.

2.1.1. Seguridad Informática

Es aquella que intenta proteger los activos de las organizaciones, estos activos pueden ser equipos físicos, aplicaciones, información, comunicaciones entre otros. Según (López, 2010) "La seguridad informática es una disciplina que involucra el diseño de reglas, procesos, métodos y técnicas para lograr sistemas de información seguros y confiables.." (p.9). Todas las empresas y organizaciones salvo algunas excepciones manejan Sistemas de información y sistemas informáticos que apoyan el funcionamiento de la organización por lo que la existencia de normas y procedimientos que permitan proteger dichos sistemas es fundamental para proteger los activos de la organización.

Existen varias definiciones que ayudan a clasificar diferentes conceptos de seguridad dependiendo de lo que se esté tratando de proteger o la forma en la que se realice la protección algunas de ellas son:

2.1.1.1. Seguridad Física

Cubre todo lo referente a equipos informáticos como computadoras, servidores, equipos de red. Las principales amenazas a las que los equipos físicos están expuestos son los robos, desastres naturales, fallos de energía entre otros.(Fabián & Buendía, 2013)

2.1.1.2. Seguridad Lógica

Hace referencia a las aplicaciones instaladas que se ejecutan en los equipos físicos o a los sistemas operativos. Las amenazas que afectan a la seguridad lógica son principalmente los diferentes tipos de virus (troyanos, malware, adware.), la pérdida de datos, ataques directos al servidor aprovechando las vulnerabilidades.(Fabián & Buendía, 2013)

2.1.1.3. Seguridad Activa

Busca la solución antes que de llegue un problema. Adopta medidas para proteger los activos de la empresa(Fabián & Buendía, 2013)

2.1.1.4. Seguridad Pasiva

Son mecanismos que protegen a la organización después de que llega un ataque, por ejemplo, una copia de seguridad no permitiría proteger la información en caso de un ataque o de que un equipo sufra algún daño.(Fabián & Buendía, 2013)

2.1.2. Seguridad de la Información

La información se define como un activo importante de un negocio, este tiene un gran valor para las organizaciones y requiere una protección adecuada. Estos se encuentran asociados a riesgos y amenazas que explotan un amplio campo de vulnerabilidades.(Organización Internacional de Normalización, 2005).

La seguridad de la información tiene relación directa con medidas preventivas que son aplicadas con el propósito de salvaguardar y proteger la información bajo la integridad, disponibilidad y confidencialidad (Solarte et al., 2015). La confidencialidad de la información se la garantiza con el acceso a esta únicamente por personal autorizado, para preservar la integridad se debe cuidar que la información no sea alterada y se mantenga tal y como desee el usuario y para conservar la disponibilidad se debe garantizar el acceso a la información por parte de los usuarios en cualquier momento que se necesite.(Fabián & Buendía, 2013). Las organizaciones tienen que aplicar metodologías que ayuden a preservar la información, este en formato físico o electrónico e implementar la tecnología necesaria para lograr este objetivo.

2.1.3. Vulnerabilidades

Según (López, 2010), las vulnerabilidades representan la posibilidad de que se cristalice una amenaza informática sobre un activo. No todos los activos son vulnerables a las mismas amenazas, por ejemplo, los datos son vulnerables al robo de información, mientras que un servidor puede ser vulnerable a un fallo eléctrico o de mantenimiento.

2.1.4. Amenazas

Son los ataques internos o externos a los que están expuestos los sistemas informáticos aprovechando sus vulnerabilidades. Una amenaza puede ser ocasionada por diversos factores como personas, máquinas o sucesos que buscan la oportunidad de producir algún daño. Hay diferentes tipos de amenazas, pero la mayoría son de carácter físico o lógico(Sena & Tenzer, 2004). Algunos ejemplos de amenazas son daños de hardware, sucesos ambientales, software malicioso, robo o destrucción de información.

2.1.5. Riesgos

Se define como la posibilidad que ocurra o no una amenaza aprovechando las vulnerabilidades del sistema. Un riesgo existe siempre y cuando existan vulnerabilidades a las que las amenazas

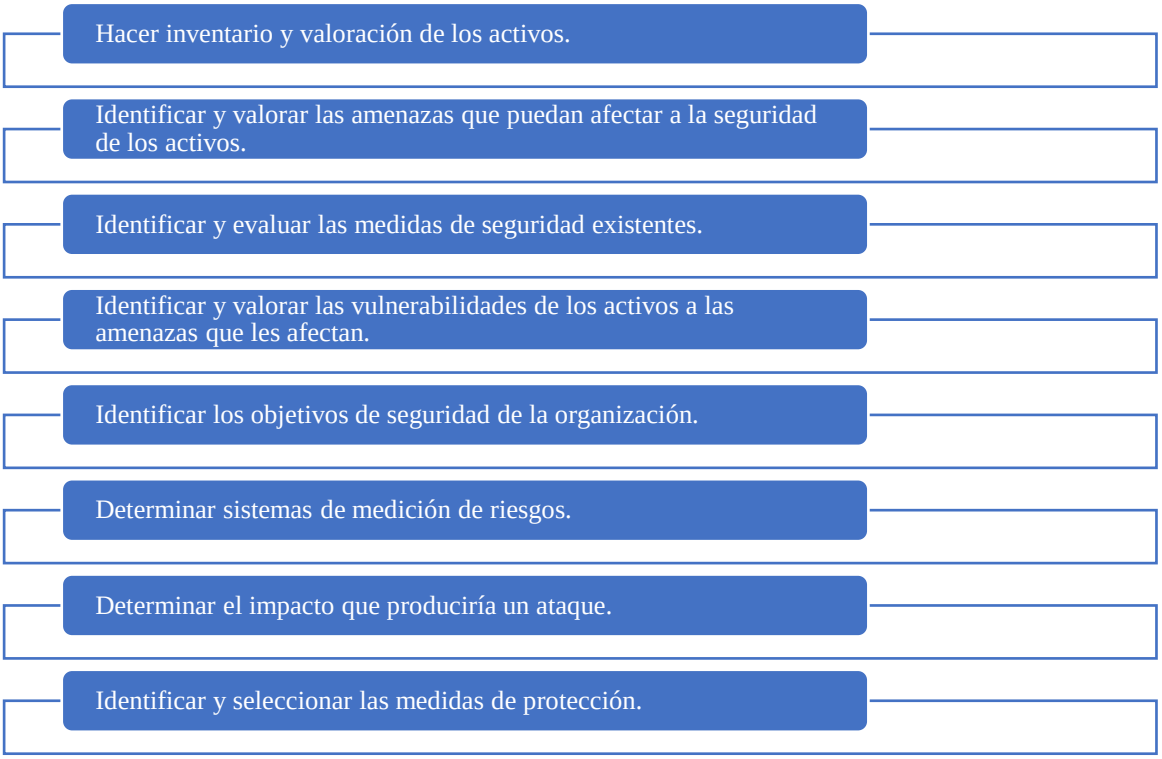
puedan atacar. Otra definición como lo describe (Talabis & Martin, 2013) el riesgo se puede definir como la cuantificación o medición de la incertidumbre, los análisis de riesgo son principalmente un ejercicio de medición de la incertidumbre.

Una organización en la que no se ha identificado o medido sus riesgos permanecerá en un estado de incertidumbre en donde no puede protegerse contra posibles peligros. Si una organización no conoce su estado de riesgo, esta no podrá protegerse contra posibles peligros hasta que sea capaz de identificarlos y medirlos.

2.2. *Análisis de Riesgos*

2.2.1. Proceso de Análisis de Riesgo

Para (López, 2010) se necesita seguir los siguientes pasos para realizar un análisis de riesgos:



2.2.2. Metodologías de Análisis de Riesgos

La norma ISO 3100 (ISO, 2018) plantea algunas metodologías de análisis de riesgo que están divididas en dos grupos principales:

2.2.2.1. Metodologías de gestión de riesgo

Están orientadas a la evaluación, identificación, y posterior tratamiento de riesgo derivados de una actividad. Algunos ejemplos son:

- Norma ISO 31000.
- Método del ARO.
- AS/NZS 4360.
- APPCC (Análisis de Peligros y Puntos Críticos de Control).

2.2.3. Metodologías de Cuantificación

Se enfocan en la cuantificación del riesgo, utilizan indicadores para medir el impacto que el riesgo pueda tener en las instituciones, con este cálculo elaboran planes para la gestión. Algunos ejemplos son:

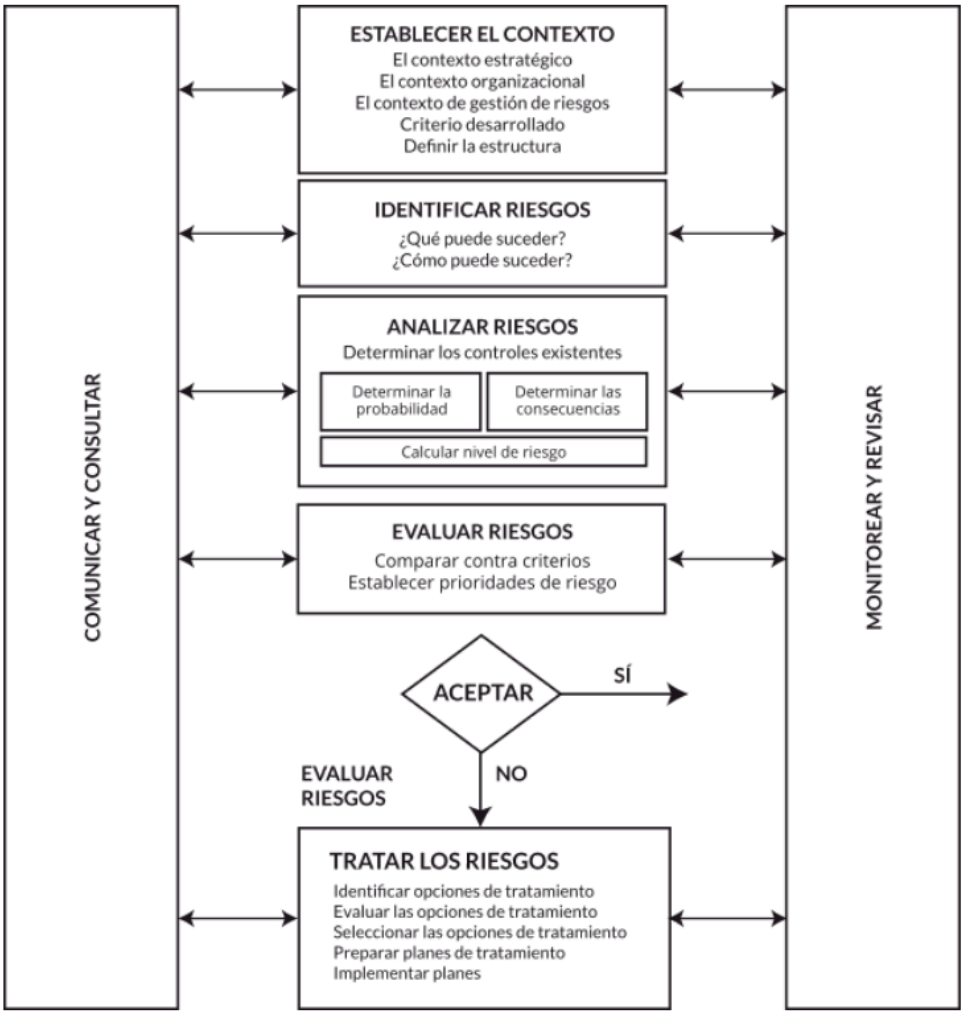
- Magerit.
- Delphi.

2.3. *Gestión de Riesgos*

Según la norma ISO 31000 la gestión de riesgos son todas las acciones realizadas de manera coordinada que orientan y controlan los riesgos que pueden estar destinados a sufrir. (ISO, 2018).

La gestión de riesgos tiene como objetivo establecer una serie de indicaciones para comprender qué aspectos hay que gestionar y cómo hacerlo. El proceso de gestión de riesgo establecido por la norma ISO 31000 esta detallado en la figura 7.

Figura 7
Proceso de Gestión de Riesgos



Nota. *La imagen muestra el proceso paso a paso a para realizar la Gestión de riesgos*
Fuente:(ISO, 2018)

La gestión de riesgos permite a los encargados de TI equilibrar los aspectos operativos y costos económicos de la implementación de medidas de protección provocando un gran beneficio hacia la organización (Talabis & Martin, 2013).

2.4. *Plan de Contingencia*

Se define como una estrategia planificada con una serie de procedimientos que faciliten tener una solución alternativa para restituir rápidamente los servicios de la institución ante cualquier eventualidad que los pueda paralizar , ya sea esta de forma total o parcial(Ignacio et al., 2015)

2.5. *PILAR*

La metodología MAGERIT puede aplicarse mediante un software de nombre PILAR. El software PILAR desarrollado por el Centro Nacional de Inteligencia– Centro Criptológico Nacional, con la colaboración del MAP, posee librerías para la aplicación de Magerit versión 3 que sirve para realizar el análisis y la gestión de riesgos.

CAPÍTULO 3

3. ANÁLISIS DE RIESGOS

Para el análisis de riesgos es necesario seguir los siguientes pasos:

1. Identificar los activos más relevantes del departamento de tecnología.
2. Identificar las amenazas a la que los activos están expuestos.
3. Estimar el impacto que pueda tener la cristalización de cualquier amenaza sobre los activos.
4. Estimar el riesgo.

3.1. *Caracterización de los Activos*

En el presente apartado se destacan 3 actividades principales que se detallan a continuación:

- Identificar los activos.
- Definir la dependencia entre activos.
- Realizar la valoración de activos.

Como actividad principal se tiene el reconocimiento de los activos que posee el departamento de tecnología, la verificación de la dependencia que existe entre ellos y la valoración que tiene cada activo.

3.1.1. Identificación de los Activos

Los activos son los recursos con los que cuenta la organización. Los activos más relevantes que se toman en cuenta en Magerit son:

- Los Datos.
- Los Servicios.
- Servicios Subcontratados.
- El software.

- Equipos Informáticos (Hardware).
- Equipamiento Auxiliar.
- Dispositivos de almacenamiento.
- Redes de comunicaciones.
- Las Instalaciones.
- El personal.

Los activos más relevantes que posee el departamento de tecnología en la EPMR se encuentran listados en el

ANEXO C IDENTIFICACIÓN DE LOS ACTIVOS**.**

3.1.2. Dependencia de los Activos

La información y los servicios son los activos esenciales en una organización, pero estos dependen directamente de otros activos como los equipos informáticos, las comunicaciones, el personal, entre otros.

Una manera de representar esta dependencia es realizando gráficos como en forma de árboles donde se van ubicando los activos de acuerdo con su importancia y a sus relaciones. Los activos que se encuentran más arriba en el árbol van a depender de los activos que están en la parte inferior.

Según (Consejo Superior de Administración Electrónica, 2012a) Un activo superior depende de otro activo inferior cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior."

Se pueden agrupar el conjunto de activos en capas en donde las capas superiores dependen de las inferiores como lo muestra en la Tabla 3 .

Tabla 3
Dependencias

Activos esenciales	Información
	Servicios
Servicios internos	
Equipos Informáticos	Software
	Hardware
	Comunicaciones
	Dispositivos de Almacenamiento
El entorno	Equipamiento y Suministros
	Mobiliario
Servicios Subcontratados	
Instalaciones Físicas	
Personal	Usuarios
	Operadores y Administradores
	Desarrolladores

Nota. Tabla de Dependencias entre activos basada en la recomendación de MAGERIT Elaborado por los Autores basados en del Libro I Magerit-versión 3.0 página 23.

El resultado del análisis de dependencias de los activos dentro de la organización se muestra en la Figura 8 en donde PILAR clasifico los activos de acuerdo a los lineamientos mostrados en la Tabla 3. Cada activo mostrado en la Figura 8 está representado por códigos cuya equivalencia se la puede encontrar encuentra en el ANEXO C IDENTIFICACIÓN DE LOS ACTIVOS donde están listados todos los activos con su respectivo código.

Figura 8
Dependencia de los activos

Nota. *Imagen que muestra la dependencia que hay entre activos basándose en el código de colores que se muestra en la imagen. Elaborado por Autores a través de PILAR.*

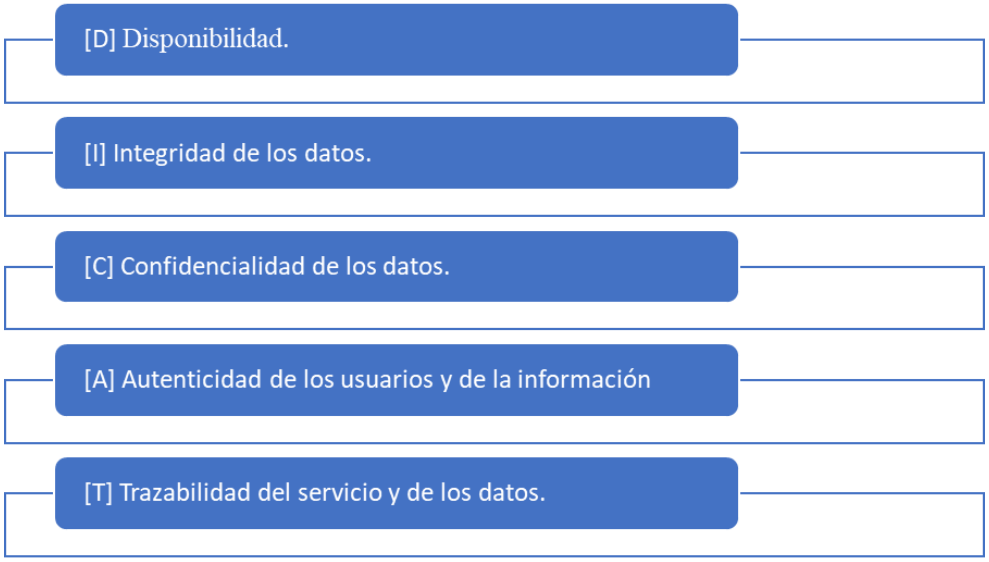
3.1.3. Valoración de un Activo

La valoración es la determinación del costo de recuperación de un evento que destruye el activo.

- Valoración cualitativa
    - Es un tipo de análisis de riesgo que permite avanzar con rapidez debido a que posicionan los activos en un orden relativo, por ejemplo, se puede valorar los activos de acuerdo la magnitud del riesgo de que ocurra una amenaza y de esta manera saber que activo vale más en comparación de otro.
- Valoración Cuantitativa
    - En la valoración cuantitativa se busca saber qué y cuanto hay, es decir, se cuantifican todos los aspectos posibles de un activo. Este modelo trabaja de manera numérica con un valor real superior a cero.
    - Para medir la valoración de una activo de acuerdo se podría utilizar valores monetarios, por ejemplo.

3.1.4. Dimensiones de valoración un activo

Son utilizadas para valorar los resultados de que una amenaza se materialice. El objetivo de esto es valorar el prejuicio que adquiere un activo en cada dimensión cuando es atacado. Las dimensiones que se toman en cuenta en Magerit son:



Para valorar las dimensiones se tiene que hacer una serie de preguntas a los encargados o a personas que conozcan el impacto que puede tener una amenaza sobre los activos. Las preguntas están listadas en la Tabla 4. .

Tabla 4.
Dimensiones de Valoración

DIMENSIÓN	PREGUNTA
Confidencialidad	¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
Integridad	¿Qué importancia tendría que los datos fueran modificados fuera de control?
Disponibilidad	¿Qué importancia tendría que el activo no estuviera disponible?
Autenticidad	¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
Trazabilidad	¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?
	¿Qué importancia tendría que no quedara constancia del acceso a los datos?

Nota. Dimensiones utilizadas para valorar a los activos. Elaborado por Autores a través de del Libro I Magerit-versión 3.0 página 24.

3.1.5. Criterios de Valoración

Una vez se tenga en claro las dimensiones que se van a valorar se puede empezar a conocer las formas o los criterios de valoración que se les va a dar a cada dimensión.

Teóricamente se puede utilizar cualquier escala de valores siempre y cuando esta sea común para todas las dimensiones, también esta debe ser logarítmica y centrada en diferencias relativas de valor, no en diferencias absolutas.

Tabla 5
Criterios de Valoración

Nivel	Criterio
10	Nivel 10
9	Nivel 9
8	Nivel 8(+)
7	Alto
6	Alto (-)
5	Medio (+)
4	Medio
3	Medio (-)
2	Bajo (+)
1	Bajo
0	Depreciable

Nota: Criterios de valoración a utilizar para valorar los activos. Elaborado por los autores basados en PILAR.

Tabla 6
Valoración de los Activos

	[D]	[I]	[C]	[A]	[T]
[B]ACTIVOS ESENCIALES					
[E1] Información Confidencial		[9]	[9]	[9]	[8]
[IS]SERVICIOS INTERNOS					
[is1] Voz sobre IP	[8]			[8]	[8]
[is2] Internet	[7]			[8]	[7]
[is3] Soporte al usuario	[7]			[3]	[7]
[is4] servidor de nombres de dominio	[7]			[7]	[7]
[SS] SERVICIOS SUBCONTRATADOS					
[ss1] impresión	[7]			[3]	[5]
[ss2] alojamiento de servidor Web	[7]			[6]	[6]
[ss3] Correo Electrónico	[7]			[7]	[7]
[ss4] proveedor de servicio de internet	[8]			[8]	[8]
[ss5] respaldo de datos	[7]			[8]	[6]
[ss6] alojamiento de aplicaciones (hosting)	[7]			[7]	[7]
[SW]APLICACIONES					
[sw1] Sistema Financiero CGWEB		[9]	[9]	[9]	[9]
[sw2] Ofimática					[7]
[sw3] servidor de directorio		[9]	[9]	[9]	[9]
[sw4] sistema de gestión de base de datos (Oracle 11g)					[7]
[sw5] sistema operativo (windows, linux)					[7]
[sw6] hipervisor (gestor de la máquina virtual)					[5]
[sw7]Sistema de Gestión Documental RUMIDOCS		[8]	[8]	[8]	[8]
[sw8] Respaldos (Acronis)					[7]
[sw9]Antivirus (ESET)					[7]
[sw10] Monitoreo de Red (PRTG)					[7]
[sw11] Sophos SSL VPN Client					[7]
[HW] EQUIPAMIENTO INFORMÁTICO					
[hw1]Servidores	[9]	[9]	[9]	[9]	[9]
[hw2] Equipos Virtuales	[9]	[9]	[9]	[9]	[9]
[hw3]Conmutador					[8]
[hw4] punto de acceso inalámbricos					[8]
[hw5] Teléfonos ip					[6]
[hw6] informática personal (Computadores Todo en Uno, computador de escritorio, laptops)					[8]
[hw1]Firewall	[9]	[9]	[9]	[9]	[9]
[COM] REDES DE COMUNICACIONES					
[com1] red telefónica		[7]			
[com2] red de datos					[7]
[com3] wifi					[7]
[com4] red local					[7]
[com5] red virtual					[7]
[com6] VPN				[8]	[8]

[SI] SOPORTES DE INFORMACIÓN					
[SI1]discos		[7]	[7]		
[SI2] memorias USB		[7]	[7]		
[SI3] material impreso		[7]	[7]		
[AUX] EQUIPAMIENTO AUXILIAR					
[aux1] Equipos de climatización	[7]				
[aux2] Fuentes de alimentación	[7]				
[aux3] cableado de datos (fibra y de alimentación)	[7]				
[aux4] sistema de alimentación interrumpida	[7]				
[aux5] sistema de video vigilancia	[7]				
[L]INSTALACIONES					
[i1] edificio			[8]		
[P]PERSONAL					
[p1]administradores de sistemas Ing. Luis Villalta – Jefe de TIC´s.			[8]		
[p2]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática			[8]		

Nota. Tabla de valoración de los activos por dimensión. Elaborado por el departamento de tecnología en conjunto con los Autores en PILAR.

- Cabe mencionar que el servicio de Internet especificado en Servicios Internos es el que se proporciona a los funcionarios de la empresa, la caída de este servicio puede causar la interrupción de actividades propias de la empresa.
- La ponderación realizada a cada activo de la tabla 6, la realizó el personal del departamento de tecnología en conjunto con los autores como se indica en el **ANEXO G VALORACIÓN DE ACTIVOS.**

3.2. *Caracterización de las Amenazas*

En esta actividad, el objetivo es realizar la identificación de las amenazas más relevantes de cada activo. Según la herramienta PILAR, estandarizada por Magerit, las amenazas se subdividen en 4 grupos:

- [N] Desastres Naturales.
- [I] De Origen Industrial.

- [E] Errores y fallos no intencionados.
- [A] Ataque intencionados.

3.2.1. Identificación de las Amenazas

El siguiente paso es identificar las causas potenciales que puedan ocasionar daños en la organización. Las amenazas típicas que se pueden encontrar pueden ser de origen natural, del entorno, defectos de las aplicaciones o causadas por el personal de forma accidental o deliberada. Para mayor detalle la Tabla 7 resume el catálogo de amenazas detalladas en el libro de MAGERIT (Consejo Superior de Administración Electrónica, 2012c).

Tabla 7
Tipos de Amenazas

Tipo de Amenaza	Descripción
De Origen Natural	▪ Fuego ▪ Daños por agua ▪ Desastres Naturales
De origen Industrial	▪ -Corte del suministro eléctrico ▪ -Condiciones inadecuadas de temperatura o humedad ▪ -Fallo de servicios de comunicaciones ▪ Desastres industriales
Errores no intencionados	▪ Fuga de información ▪ Errores de los usuarios ▪ Introducción de falsa información ▪ Errores del administrador ▪ Acceso no autorizado ▪ Errores de configuración ▪ Vulnerabilidad de programas (software) ▪ Degradación de los soportes de almacenamiento de la información ▪ Corrupción de la información ▪ Difusión de software dañino ▪ Destrucción de información ▪ Errores de mantenimiento / actualización de programas (software) ▪ Interceptación de información (escucha) ▪ Errores de mantenimiento / actualización de equipos (hardware) ▪ Indisponibilidad del personal ▪ Caída del sistema por sobrecarga ▪ Agotamiento de recursos
Ataque Intencionados	▪ Denegación de servicio ▪ Robo ▪ Ataques destructivos ▪ Extorsión ▪ Ingeniería social ▪ Manipulación de logs ▪ Abuso de privilegios de acceso ▪ Manipulación de equipos ▪ Manipulación de configuración ▪ Alteración de la información

Nota. Catálogo de Amenazas de MAGERIT. Elaborado por los Autores, a través del Libro II Magerit-versión 3.0 página 25.

Una vez que se conocen el catálogo se procede a clasificar por activo cada una de las posibles amenazas que los puedan afectar. La tabla completa con las amenazas por cada activo se encuentra en el ANEXO D AMENAZAS SOBRE CADA ACTIVO.

3.2.2. Valoración de las Amenazas

Una vez determinadas las amenazas estas se evalúan de acuerdo con la influencia que puede tener sobre el activo. Se toman dos parámetros para valorar las amenazas que son la degradación y la probabilidad:

Degradación: Mide el daño que puede ocasionar una amenaza sobre un activo en caso de que ocurra. La Figura 9 muestra la escala a utilizar para valorar la degradación que puede tener el activo.

Figura 9
Valoraciones para la Degradación

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Nota. Valores para calificar la degradación de los activos debido a las amenazas. Fuente: (Consejo Superior de Administración Electrónica, 2012a)

Para valorar la degradación se tomará en cuenta el daño que puede provocar una amenaza sobre la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad que corresponda a cada activo.

Probabilidad: ¿Qué tan probable es que ocurra la amenaza? Se la puede medir de manera numérica tomando en cuenta la frecuencia en la que ocurre o puede ocurrir. Se utilizarán los valores mostrados en la Figura 10

Figura 10

Valores para la Probabilidad

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

Nota. Valores para calificar la degradación de los activos debido a las amenazas. Fuente: (Consejo Superior de Administración Electrónica, 2012a)

La valoración de todas las amenazas en degradación y probabilidad de ocurrencia se encuentra en el **ANEXO E VALORACIÓN DE LAS AMENAZAS.**

3.3. *Valores Acumulados y Repercutidos*

Según MAGERIT se puede calcular el impacto y el riesgo tanto de manera acumulada como repercutida, estas tienen sus diferencias que están descritas en la Tabla 8

y en la Tabla 9

Tabla 8

Diferencias entre Impacto Acumulado y Repercutido

Impacto Acumulado	Impacto Repercutido
Es el calculado sobre un activo teniendo en cuenta • su valor acumulado (el propio más el acumulado de los activos que dependen de él) • las amenazas a que está expuesto	Es el calculado sobre un activo teniendo en cuenta • su valor propio • las amenazas a que están expuestos los activos de los que depende
El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.	El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.
El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo	El impacto es tanto mayor cuanto mayor es el valor propio de un activo.
El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.	El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.
	El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.
El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.	El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Nota. Comparación entre Impacto Acumulado y Repercutido Elaborado por Autores, a través del Libro I Magerit-versión 3.0 página 28.

Tabla 9

Comparación Riesgo Acumulado vs Repercutido

Riesgo Acumulado	Riesgo Repercutido
Es el calculado sobre un activo teniendo en cuenta • el impacto acumulado sobre un activo debido a una amenaza y • la probabilidad de la amenaza	Es el calculado sobre un activo teniendo en cuenta • el impacto repercutido sobre un activo debido a una amenaza y • la probabilidad de la amenaza
El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.	El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza
El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.	El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Nota. Comparación entre Riesgo Acumulado y Repercutido. Elaborado por Autores, a través del Libro I Magerit-versión 3.0 página 30.

Los valores que se van a tomar en cuenta para posterior uso son los valores acumulados debido a que muestran de una manera general el impacto y el riesgo actual de cada activo sobre la organización. Estos valores permiten determinar las salvaguardas que se van a utilizar.

3.4. *Estimación del estado de riesgo*

Esta tarea se centra en determinar un estimado del estado de riesgo que el departamento de tecnología tiene actualmente.

Esta actividad consta de dos subactividades que se detallan a continuación:

- Evaluación del impacto.
- Evaluación del riesgo.

Durante esta actividad como objetivo principal se debe de tener en claro lo que puede llegar a ocurrir (impacto) y de lo que posiblemente pueda ocurrir en este caso (riesgo).

3.4.1. Determinación del impacto potencial

Es la medida del daño que afecta al activo provocado por la cristalización de una amenaza(Consejo Superior de Administración Electrónica, 2012a). Una vez se conoce el valor de los activos y la degradación causada por las amenazas se puede realizar una matriz para medir el impacto basándose en el ejemplo de la Figura 11 .

Figura 11
Matriz Impacto Potencial

impacto		degradación		
		1%	10%	100%
valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

- MB: muy bajo.
- B: bajo.
- M: medio.
- A: alto.
- MA: muy alto.

Nota. Ejemplo de Matriz de Impacto Potencial recomendada por MAGERIT. Fuente: (Consejo Superior de Administración Electrónica, 2012a)

En caso de que un activo reciba una calificación de MA este debe ser atendido de forma inmediata.(Consejo Superior de Administración Electrónica, 2012b).

Figura 12
Escala Impacto Potencial PILAR

MB: muy bajo	[1] Bajo [0] Despreciable
B: bajo	[3] Medio(-) [2] Bajo(+)
M: medio	[5] Medio(+) [4] Medio
A: alto	[7] Alto [6] Alto(-)
MA: muy alto	[10] Nivel 10 [9] Nivel 9 [8] Alto(+)

Nota. Escala de impacto potencial y su equivalencia en código de colores. Elaborado por Autores en PILAR

El impacto potencial de cada activo sobre la disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A) y trazabilidad (T) calculado por PILAR teniendo en cuenta el valor de los activos y la degradación que provocan las amenazas se encuentra en la En el caso de la Tabla 10 se utiliza la escala que se muestra en la Figura 12

obtenida directamente del programa PILAR. La escala de valores va de cero

hasta diez teniendo en cuenta el impacto desde, muy bajo hasta muy alto con su respectivo código de color.

Tabla 10

En el caso de la Tabla 10 se utiliza la escala que se muestra en la Figura 12 obtenida directamente del programa PILAR. La escala de valores va de cero hasta diez teniendo en cuenta el impacto desde, muy bajo hasta muy alto con su respectivo código de color.

Tabla 10
Impacto Potencial

	D	I	C	A	T
[B]ACTIVOS ESENCIALES					
[E1] Información Confidencial	9	9	8		
[IS]SERVICIOS INTERNOS					
[is1] Voz sobre IP	6	6	6	6	
[is2] Internet	3	3	3		
[is4] Soporte al usuario	6	6	6		
[is3] servidor de nombres de dominio	8	8	8		
[SS] SERVICIOS SUBCONTRATADOS					
[ss1] impresión	6	8	6		
[ss2] alojamiento de servidor Web	8	8	8		
[ss3] Correo Electrónico	6	3	6		
[ss4] proveedor de servicio de internet	6	3	3		
[ss5] respaldo de datos	4	3	6		
[ss6] alojamiento de aplicaciones (hosting)	6	3	3		
[SW] APLICACIONES					
[sw1] Sistema Fianciero CGWEB	8	6	6		
[sw2] Ofimática	6	6	6		
[sw3] servidor de directorio	6	6	6	6	
[sw4] sistema de gestión de base de datos (Oracle 11g)	8	6	6		
[sw5] sistema operativo (windows, linux)	6	6	6		
[sw6] hipervisor (gestor de la máquina virtual)	6	3	6		
[sw7]Sistema de Gestión Documental RUMIDOCS	6	6	6	6	
[sw8] Respaldos (acronis)	8	6	6		
[sw9]Antivirus (ESET)	8	6	6	6	
[sw10] Monitoreo de Red (PRTG)	6	6	6	6	
[sw11] Sophos SSL VPN Client	8	6	6	6	

[HW] EQUIPAMIENTO INFORMÁTICO					
[hw1]Servidores	9	8	8		
[hw2] Equipos Virtuales	8	3	6		
[hw3]Conmutador	6				
[hw4] punto de acceso inalambricos	8				
[hw5] teléfonos ip	6	8	8		
[hw6] informática personal (Computadores Todo en Uno, computador de escritorio, laptops)	6	6	6		
[hw7] Firewall	9	8	8		
[COM] REDES DE COMUNICACIONES					
[com1] red telefonica	6		8		
[com2] red de datos	6	6	6		
[com4] wifi	6		3		
[com5] red local	3	6	6	6	
[com6] red virtual	6	6	6		
[com3] VPN	3			5	
[SI] SOPORTES DE INFORMACIÓN					
[SI1]discos		3	6		
[SI2] memorias USB		8	8		
[SI3] material impreso		3	6		
[AUX] EQUIPAMIENTO AUXILIAR					
[aux1] Equipos de climatización	6				
[aux2] Fuentes de alimentación	6				
[aux3] cableado de datos (fibra y de alimentación)	8				
[aux4] sistema de alimentación interrumpida	6				
[aux5] sistema de video vigilancia	6				
[L]INSTALACIONES					
[i1] edificio	8				
[P]PERSONAL					
[p2]administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.	6	8	8		
[p1]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática	6	8	8		

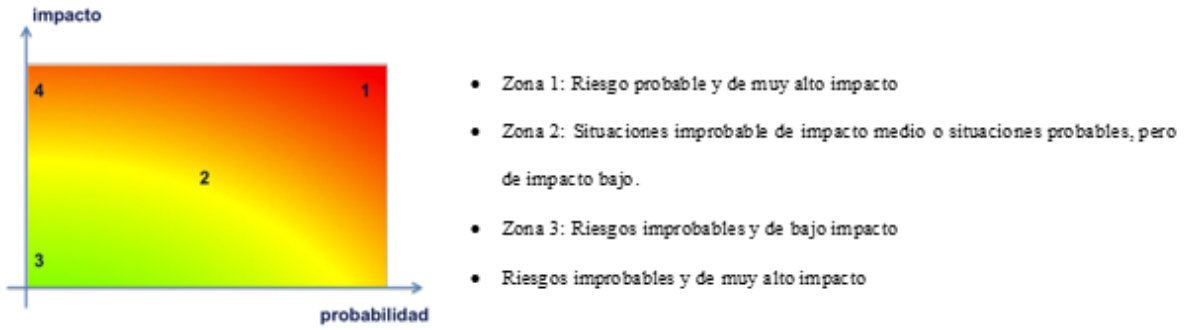
Nota: Impacto potencial calculado por PILAR. Elaborado por Autores en PILAR

3.4.2. Determinación del riesgo potencial

El riesgo se mide conociendo el impacto de las amenazas sobre los activos y la probabilidad de que se materialicen. Como se puede ver en la Figura 12

mientras más alto el impacto y la probabilidad mayor es el riesgo.

Figura 13
Determinación Riesgo Potencial



Nota. El riesgo en función del impacto y la probabilidad. Fuente: (Consejo Superior de Administración Electrónica, 2012a)

Otra forma de representar el riesgo potencial según (Consejo Superior de Administración Electrónica, 2012a), está representada en la matriz de la Tabla 11 que muestra de manera más clara la incidencia del impacto y la probabilidad sobre la gravedad del riesgo.

Tabla 11
Cálculo Riesgo Potencial

riesgo		***probabilidad***				
		MB	B	M	A	MA
impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Nota. *Tabla ejemplo para determinar el riesgo potencial. Fuente: (Consejo Superior de Administración Electrónica, 2012b).*

En donde las escalas son:

Tabla 12
Escala Riesgo Potencial

escalas		
impacto	probabilidad	riesgo
MA: muy alto	**MA:** prácticamente seguro	**MA:** crítico
A: alto	**A:** probable	**A:** importante
M: medio	**M:** posible	**M:** apreciable
B: bajo	**B:** poco probable	**B:** bajo
MB: muy bajo	**MB:** muy raro	**MB:** despreciable

Nota. Escala de equivalencias para interpretar la tabla de riesgo potencial. Fuente:(Consejo Superior de Administración Electrónica, 2012b)

En el caso del proyecto el programa PILAR luego de calcular el resigo de cada activo usa la escala de valor de la Figura 14 para representar el riesgo potencial.

Figura 14
Escala de Valor Riesgo Potencial

Nota. Escala de valor con colores para interpretar el riesgo potencial. Fuente: PILAR

El riesgo potencial de cada activo sobre la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad se muestra en la

Tabla 13 , es la valoración del riesgo a la que están expuestos los activos sin salvaguardas.

Tabla 13
Riesgo Potencial

	D	I	C	A	T
[B] ACTIVOS ESENCIALES					
[E1] Información Confidencial	5,4	5,4	4,8		
[IS] SERVICIOS INTERNOS					
[is1] Voz sobre IP	5,4	5,4	5,4	3,6	
[is2] Internet	1,8	1,8	1,8		
[is4] Soporte al usuario	3,6	4,5	4,5		
[is3] servidor de nombres de dominio	5,7	5,7	5,7		
[SS] SERVICIOS SUBCONTRATADOS					
[ss1] impresión	5,4	6,6	5,4		
[ss2] alojamiento de servidor Web	5,7	5,7	5,7		
[ss3] Correo Electrónico	4,5	1,8	4,5		
[ss4] proveedor de servicio de internet	3,6	1,8	1,8		
[ss5] respaldo de datos	3,3	2,7	3,6		
[ss6] alojamiento de aplicaciones (hosting)	4,5	1,8	1,8		
[S]WAPLICACIONES					
[sw1] Sistema Fianciero CGWEB	5,7	4,5	4,5		
[sw2] Ofimática	4,5	4,5	4,5		
[sw3] servidor de directorio	4,5	4,5	4,5	3,6	
[sw4] sistema de gestión de base de datos (Oracle 11g)	5,7	4,5	4,5		
[sw5] sistema operativo (windows, linux)	4,5	4,5	4,5		
[sw6] hipervisor (gestor de la máquina virtual)	4,5	2,7	3,6		
[sw7]Sistema de Gestión Documental RUMIDOCS	4,5	4,5	4,5	3,6	
[sw8] Respaldos (acronis)	5,7	4,5	3,6		
[sw9]Antivirus (ESET)	5,7	4,5	4,5	3,6	
[sw10] Monitoreo de Red (PRTG)	4,5	4,5	3,6	3,6	
[sw11] Sophos SSL VPN Client	5,7	4,5	3,6	3,6	
[HW] EQUIPAMIENTO INFORMÁTICO					
[hw1]Servidores	6,2	4,8	4,8		
[hw2] Equipos Virtuales	6,6	2,7	2,7		
[hw3]Conmutador	4,5				
[hw4] punto de acceso inalambricos	5,7				
[hw5] teléfonos ip	4,5	5,7	5,7		
[hw6] informática personal (Computadores Todo en Uno, computador de escritorio, laptops)	4,5	3,7	4,5		
[hw7] Firewall	6,2	4,8	4,8		
[COM] REDES DE COMUNICACIONES					
[com1] red telefonica	4,5		5,7		
[com2] red de datos	3,6	3,6	3,6		
[com4] wifi	4,5		2,7		
[com5] red local	1,8	4,5	4,5	4,5	
[com6] red virtual	3,6	3,6	4,5		
[com3] VPN	1,8			3,0	
[SI] SOPORTES DE INFORMACIÓN					
[SI1]discos		1,8	4,5		
[SI2] memorias USB		1,8	4,5		
[SI3] material impreso		1,8	3,6		
[AUX] EQUIPAMIENTO AUXILIAR					
[aux1] Equipos de climatización	4,5				
[aux2] Fuentes de alimentación	4,5				
[aux3] cableado de datos (fibra y de alimentación)	4,8				
[aux4] sistema de alimentación interrumpida	3,6				
[aux5] sistema de video vigilancia	3,6				
[L]INSTALACIONES					
[i1] edificio	5,7				
[P]PERSONAL					
[p2]administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.	3,6	5,7	4,8		
[p1]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática	3,6	5,7	4,8		

Nota: Riesgo potencial elaborado en la herramienta PILAR Elaborado por: Autores en PILAR

Los resultados presentados en la

Tabla 10 y la **¡Error! No se encuentra el origen de la referencia.** hacen referencia al cálculo del impacto y riesgo sin tomar en cuenta las salvaguardas ya implementadas, por lo que no reflejan el estado actual del área de tecnología.

3.5. *Caracterización de las Salvaguardas*

Las salvaguardas son los procedimientos o mecanismos tecnológicos de protección ante los riesgos e impactos a los que están expuestos los activos, se comprende como salvaguarda a todo aquel mecanismo que ayuda a reducir el riesgo, esta etapa es fundamental para definir cómo se pueden controlar los riesgos a los que está expuestos los activos del departamento de tecnología.

Esta actividad consta de dos subactividades que se detallan a continuación:

- Identificación de salvaguardas existentes.
- Valoración de salvaguardas existentes.

Durante esta actividad se identifica las salvaguardas pertinentes que pueden aplicarse dentro del área de tecnología, así mismo como su eficacia que ayude a la mitigación del riesgo.

Con la ayuda de la herramienta PILAR, se seleccionan las salvaguardas pertinentes que permitan contrarrestar a las amenazas identificadas, de igual manera se tomará en cuenta la sugerencia de las etapas del programa para establecer y tener claro la situación actual y la situación que se aspira alcanzar con las salvaguardas, siendo así se detallan a continuación las siguientes etapas:

- Potencial (situación actual sin salvaguardas).
- Current (Situación actual con salvaguardas existentes).
- Target (Objetivo al que se desea llegar).

3.5.1. Identificación de salvaguardas

En esta subactividad se identifican salvaguardas pertinentes para reducir el riesgo, para ello se usará la herramienta PILAR, que permite la asignación de salvaguardas a todos los activos en sus distintas dimensiones.

La herramienta PILAR únicamente recomienda aplicar las salvaguardas más relevantes, dependiendo de la necesidad que se tenga, esto quiere decir que puede omitir algunas de las salvaguardas que se tiene en la herramienta.

3.5.2. Valoración de las salvaguardas

En esta subactividad se hará énfasis en valorar las salvaguardas existentes usando en la herramienta PILAR.

3.5.2.1. ASPECTO DE SEGURIDAD

Las salvaguardas cuentan con aspectos de seguridad dependiendo a donde va dirigido, la Tabla 14 proporciona los aspectos de seguridad que usa PILAR:

Tabla 14
Aspectos de seguridad de las salvaguardas

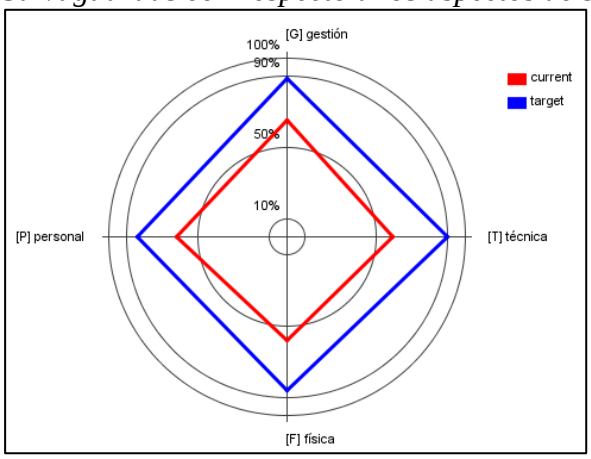
[G]	**Gestión de la seguridad**
[P]	Normativa del personal
[T]	Soluciones Técnicas: software, hardware, comunicaciones, …
[F]	Seguridad física

Nota. Aspecto de seguridad a tomar en cuenta para la implementación de salvaguardas. Elaborado por los Autores.

La Figura 15 representa gráficamente los aspectos de seguridad cubiertos actualmente vs el objetivo una vez implementada las salvaguardas.

Figura 15

Salvaguardas con respecto a los aspectos de seguridad



Nota. Salvaguardas con respecto a los aspectos de seguridad actual vs objetivo. Fuente: PILAR

3.5.2.2. ESTRATEGIA PARA REDUCIR EL RIESGO

Como alternativa a no poder evitar el riesgo, se sabe que las salvaguardas mitigan el riesgo, con dos aspectos fundamentales, el primero reduciendo la probabilidad, y el segundo reduciendo la degradación, esto con el propósito de limitar el daño.

El programa PILAR establece las estrategias que se mencionan en la Figura 16

.

Figura 16

Estrategias para reducción de riesgo

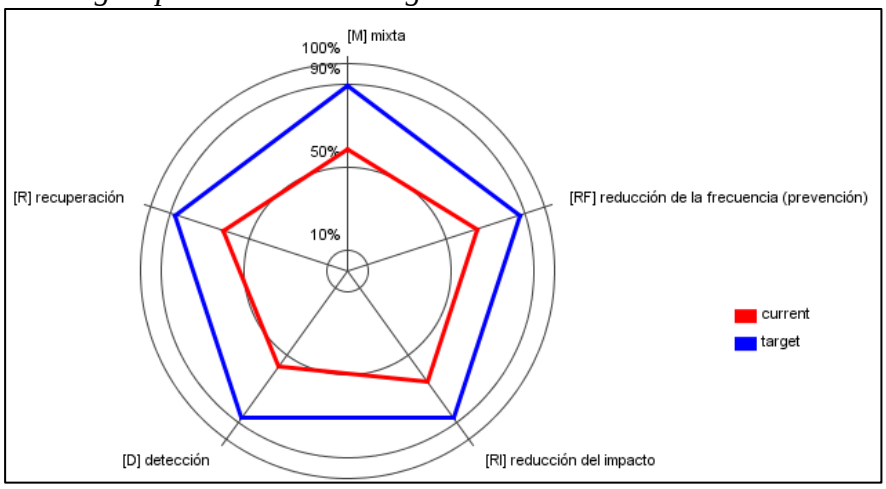
- [M] Mixta
- [RF] Reducción de frecuencia (prevención)
- [RI] Reducción de Impacto
- [D] Detección
- [R] Recuperación

Nota. Lista de estrategias de reducción de riesgo recomendadas por MAGERIT. Fuente: (Consejo Superior de Administración Electrónica, 2012a)

Una vez implementadas la salvaguarda se provee que aumenten el porcentaje de estrategias para reducir el riesgo. El aumento esperado se refleja en la Figura 17

.

Figura 17
Estrategias para reducir el riesgo



Nota. Estrategia para reducir el riesgo actual y el riesgo esperado. Elaborado por autores en PILAR

3.5.2.3. TIPO DE PROTECCIÓN

De igual manera cada salvaguarda se ve identificada con un tipo de protección, que deben estar reflejados a lo largo del proyecto en cada salvaguarda, los tipos de protección se detallan a en la Tabla 15

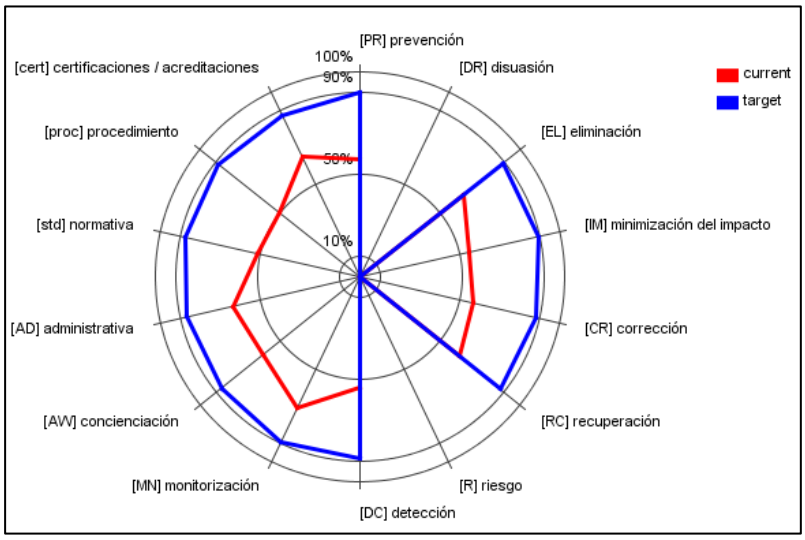
Tabla 15
Tipos de Protección

[AD]	Administrativa
[DT]	Detección
[PR]	Prevención
[CR]	Corrección
[EL]	Eliminación
[IM]	Minimización del Impacto
[DR]	Disuasión
[RC]	Recuperación
[MN]	Monitorización
[AW]	Concientización

Nota. Tipos de protección para la implementación de salvaguardas. Elaborado por Autores, a través del Libro I Magerit-versión 3.0 página 32.

Ejemplo de Tipo de protecciones

Figura 18
Ejemplo de Tipo de protecciones.



Nota. Ejemplo brindado por PILAR. Fuente Pilar

Los niveles de madurez son utilizados en la herramienta PILAR para la evaluación de las salvaguardas, estos son usados para valorar la madurez de los procesos, la parametrización de los niveles de madurez se detalla a continuación:

Tabla 16
Niveles de Madurez

EFICACIA	NIVEL	MADUREZ	ESTADO
0%	L0	Inexistente	Inexistente
10%	L1	Inicial/ad hoc	Iniciado
50%	L2	Reproducible, pero no intuitivo	Parcialmente realizado
90%	L3	Proceso definido	En funcionamiento
95%	L4	Gestionado y medible	Monitorizado
100%	L5	Optimizado	Mejora continua

Nota. Niveles de madurez en eficacia, nivel, madurez y estado. Elaborado por: Los autores, a través del Libro III Magerit-versión 3.0 página 34.

En la Figura 19 de valoración de las salvaguardas, se tiene las siguientes columnas de izquierda a derecha:

Aspecto: hace referencia a los aspectos de seguridad de las salvaguardas.

Tdp: Hace referencia al tipo de protección de la salvaguarda.

Recomendación: Valor de la salvaguarda que recomienda la aplicación. (valor de 0-10)

Salvaguarda: Hace referencia a la salvaguarda recomendada.

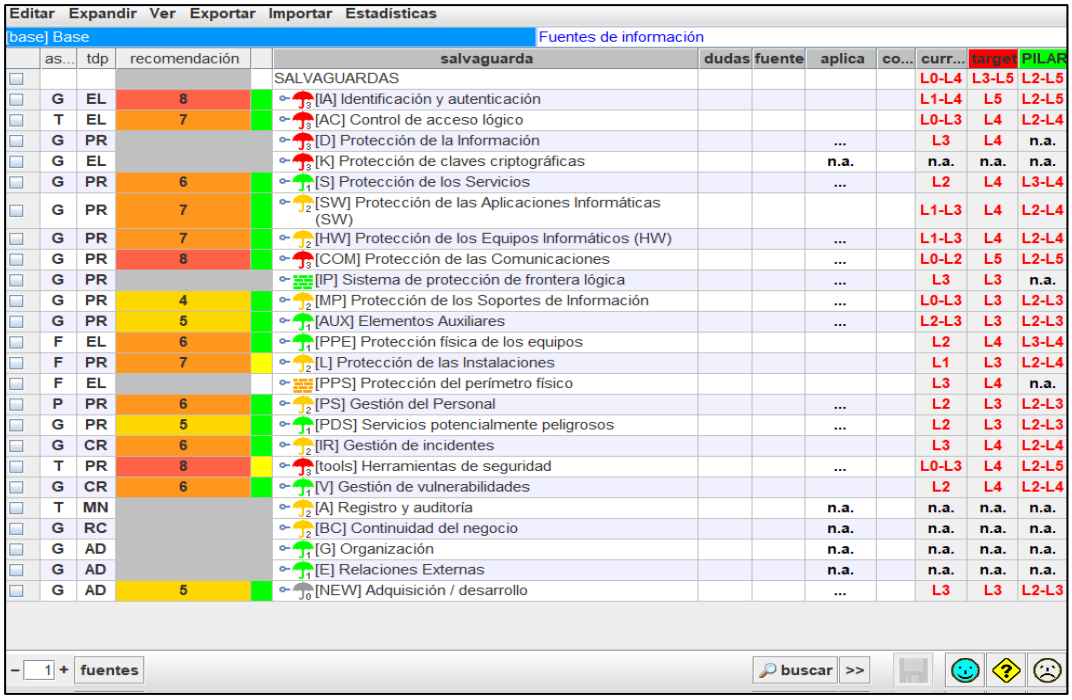
Aplica: Hace referencia a si la salvaguarda es aplicada o no.

Current: Situación actual en nivel de madurez.

Target: Objetivo a alcanzar en nivel de madurez.

Figura 19

Valoración de las salvaguardas



Editar Expandir Ver Exportar Importar Estadísticas

[base] Base | Fuentes de información

	as...	tdp	recomendación	salvaguarda	dudas	fuente	aplica	co...	curr...	target	PILAR
				SALVAGUARDAS					L0-L4	L3-L5	L2-L5
	G	EL	8	[IA] Identificación y autenticación					L1-L4	L5	L2-L5
	T	EL	7	[AC] Control de acceso lógico					L0-L3	L4	L2-L4
	G	PR		[D] Protección de la Información			...		L3	L4	n.a.
	G	EL		[K] Protección de claves criptográficas			n.a.		n.a.	n.a.	n.a.
	G	PR	6	[S] Protección de los Servicios			...		L2	L4	L3-L4
	G	PR	7	[SW] Protección de las Aplicaciones Informáticas (SW)					L1-L3	L4	L2-L4
	G	PR	7	[HW] Protección de los Equipos Informáticos (HW)			...		L1-L3	L4	L2-L4
	G	PR	8	[COM] Protección de las Comunicaciones			...		L0-L2	L5	L2-L5
	G	PR		[IP] Sistema de protección de frontera lógica			...		L3	L3	n.a.
	G	PR	4	[MP] Protección de los Soportes de Información			...		L0-L3	L3	L2-L3
	G	PR	5	[AUX] Elementos Auxiliares			...		L2-L3	L3	L2-L3
	F	EL	6	[PPE] Protección física de los equipos					L2	L4	L3-L4
	F	PR	7	[L] Protección de las Instalaciones					L1	L3	L2-L4
	F	EL		[PPS] Protección del perímetro físico					L3	L4	n.a.
	P	PR	6	[PS] Gestión del Personal			...		L2	L3	L2-L3
	G	PR	5	[PDS] Servicios potencialmente peligrosos			...		L2	L3	L2-L3
	G	CR	6	[IR] Gestión de incidentes					L3	L4	L2-L4
	T	PR	8	[tools] Herramientas de seguridad			...		L0-L3	L4	L2-L5
	G	CR	6	[V] Gestión de vulnerabilidades					L2	L4	L2-L4
	T	MN		[A] Registro y auditoría			n.a.		n.a.	n.a.	n.a.
	G	RC		[BC] Continuidad del negocio			n.a.		n.a.	n.a.	n.a.
	G	AD		[G] Organización			n.a.		n.a.	n.a.	n.a.
	G	AD		[E] Relaciones Externas			n.a.		n.a.	n.a.	n.a.
	G	AD	5	[NEW] Adquisición / desarrollo			...		L3	L3	L2-L3

– 1 + fuentes | buscar >>

Nota. Niveles de madurez calificados por cada salvaguarda. Elaborado por los autores en PILAR.

En la Figura 19 , se ingresó los niveles de seguridad de salvaguardas actual (Current) obteniendo niveles que van desde L0-L4, en donde un L0 significa que no existe una salvaguarda desplegada, con L1 las salvaguardas existen pero no se las aplican, con L2 depende mucho de la suerte, no hay un plan para los incidentes, con L3 se gestiona las salvaguardas y el éxito va más allá de la buena suerte, con L4 se controla efectividad y eficacia de las salvaguardas y con L5 se enfoca en mejora continua.

En la columna objetivo que se desea alcanzar (Target), se indica los niveles de madurez a los que se desea llegar, si bien es cierto lo óptimo es alcanzar un nivel de madurez L5, en este caso se adoptará la recomendación de PILAR para establecer un objetivo, lo esencial es obtener una mejora en los procesos hasta poder llegar a un nivel de madurez aceptable para la continuidad del correcto desempeño de la empresa.

A continuación, se indican de manera más detallada las salvaguardas implementadas, los tipos de activos involucrados, su valoración en niveles de seguridad basado en la escala de la Tabla 16 y las acciones propuestas para que para alcanzar el nivel de madurez propuesto en el target.

- **Identificación y autenticación:**

  Activos: [sw] Software

  Niveles de seguridad (L1-L4)

  - Establecer un procedimiento para resguardar la información de cada funcionario con el objeto de eliminar o bloquear cuentas de usuario que se encuentren obsoletas para la empresa.
  - Aplicar perfiles de seguridad.
  - Controlar las acciones de los usuarios para evitar ataques a otros sistemas.

- **Control de acceso Lógico:**

  Activos: [sw] Software, [com] Comunicaciones.

  Niveles de seguridad: (L0-L3).

  - Definir una política que permita controlar y gestionar el acceso lógico a los diferentes activos de información, validando la autentificación y autorización de cada funcionario.

- **Protección de la Información:**

  Activos: [B] Información.

  Niveles de seguridad: (L3).

  - Aseguramiento de la integridad de la información.
  - Analizar la frecuencia con la que se realizar copias de seguridad.
  - Definir una política para el bloqueo de puertos y evitar que la fuga de la información de la empresa por medio de pendrives.

- **Protección de los servicios:**

  Activos: [S] Servicios.

  Niveles de seguridad: (L3).

  - Seguimiento al aseguramiento de la disponibilidad de los servicios.
  - Tomar medidas frente a ataques que han sido originados dentro de la organización.
  - Garantizar la continuidad de operaciones.

- **Protección de las aplicaciones informáticas SW:**

  Activos: [sw] Aplicaciones.

  Niveles de seguridad: (L1-L3).

  - Establecer como buena práctica el realizar pruebas de actualizaciones tanto en servidores, equipos de cómputo y equipos de comunicación, previo a su instalación con el objeto de realizar un seguimiento para verificar el comportamiento de compatibilidad con las distintas aplicaciones.
  - Considerar la desactivación de actualizaciones automáticas en los equipos si así se lo considera.

- **Protección de los equipos informáticos HW:**

  Activos: [HW] Equipamiento Informático**.**

  Niveles de seguridad: (L1-L3).

  - Brindar seguimiento para el cumplimiento del correcto uso de los equipos informáticos.
  - Hacer uso de candados o cables de seguridad para equipos portátiles o computadores, con el fin de evitar su robo.

- Aplicar perfiles de seguridad, asignar cuentas con contraseñas complejas, cambiar contraseñas periódicamente para mitigar el riesgo de acceso no autorizado por parte de usuarios comunes.
- Garantizar la disponibilidad del hardware.

- **Protección de las comunicaciones:**

  Activos: [com] Redes de Comunicaciones**.**

  Niveles de seguridad: (L0-L2).

  - Implementar seguridad Wireless (WiFi).
  - Realizar copias de seguridad de las claves de autenticación.
  - Aseguramiento de la disponibilidad de las operaciones.
  - Implementar la redundancia de los enlaces con balanceo de carga.
  - Instalación de herramientas antispyware.
  - Establecer una normativa sobre el uso adecuado del servicio de Internet.
  - Autenticación de canal.

- **Sistema de protección de frontera lógica:**

  Activos: [HW] Equipamiento Informático.

  Niveles de seguridad: (L3).

  - Aplicar perfiles de seguridad.
  - Protección de la integridad en el intercambio de datos.
  - Aseguramiento de la disponibilidad.
  - Autenticación de canal.

- **Protección de los soportes de la información:**

  Activos: [media] Soportes de información.

  Niveles de seguridad: (L0-L3).

- Protección criptográfica del contenido, implementar cifrado en cuanto al almacenamiento de datos.

- **Elementos Auxiliares:**

  Activos: [aux] Equipamiento Auxiliar**.**

  Niveles de seguridad: (L2-L3).

  - Considerar la implementación de un sistema de alimentación de respaldo eléctrico.
  - Ejecutar un mantenimiento regular del cableado de datos.
  - Controlar regularmente la temperatura en los centros de datos.
  - Controlar regularmente la humedad en los centros de datos.

- **Protección física de los equipos:**

  Activos: [HW] Equipamiento Informático, [media] Soporte de Información.

  Niveles de seguridad: (L2).

  - Protección de los equipos dentro de la institución.

- **Protección de las instalaciones:**

  Activos: [L] Instalaciones.

  Niveles de seguridad: (L1).

  - Emplear un plan de protección.
  - Emplear un plan de emergencia.
  - Controlar los accesos físicos a las instalaciones permitidas.
  - Implementación de un sistema de alarma.

- **Protección del perímetro físico:**

  Activos: [L] Instalaciones.

  Niveles de seguridad: (L3).

  - Protección de las instalaciones.

- Aseguramiento de la disponibilidad.
- Control de los accesos físicos.

- **Gestión del personal:**

  Activos: [p] Personal.

  Niveles de seguridad: (L2).

  - Establecer normas para la contratación de personal, firmar acuerdos de confidencialidad de los datos.
  - Trabajar en conjunto con Talento Humano para conocer más al personal, en el caso de contratar un administrador en TI debido a que este perfil sería diferente al de un administrativo.

- **Servicios potencialmente peligrosos:**

  Activos: [S] Servicios.

  Niveles de seguridad: (L2).

  - Aplicar perfiles de seguridad.
  - Aseguramiento de la disponibilidad de los servicios.
  - Garantizar la continuidad de las operaciones.

- **Gestión de incidentes:**

  Activos: [IGR] Gestión de Incidentes.

  Niveles de seguridad (L3).

  - Establecer un proceso habitual de gestión de incidentes.

- **Herramientas de seguridad:**

  Activos: [HW] Hardware.

  Niveles de seguridad (L0-L3).

  - Implementar sistemas de detección IDS y prevención IPS.

- Implementar el monitoreo de integridad de archivos para detectar cambio o modificación en los archivos.

- **Gestión de vulnerabilidades:**

  Activos: [SW] Software.

  Niveles de seguridad (L2).

  - Emplear herramientas para la gestión y análisis de vulnerabilidades.

- **Adquisición / Desarrollo:**

  Activos: [SW] Software.

  Niveles de seguridad: (L3).

  - Establecer procesos para la Adquisición / Desarrollo de servicios.
  - Establecer procesos para la Adquisición / Desarrollo de aplicaciones.

3.6. *Impacto Residual*

A diferencia del riesgo potencial, el riesgo residual es calculado a partir de la aplicación de las salvaguardas planteadas en la sección anterior. Para calcular el impacto residual se utilizan las mismas amenazas y los mismos activos con una diferente magnitud de degradación provocada por la aplicación de las salvaguardas resultando la baja del nivel de impacto de las amenazas sobre la organización.

Figura 20
Escala de colores del Impacto Residual

Nota. Código de colores para interpretar el Impacto Residual. Fuente: PILAR

En el caso de este trabajo se tomará el impacto residual como el equivalente al impacto Current obtenido de PILAR, que está representado en la Tabla 17 Impacto Residual teniendo en cuenta la escala de la Figura 20

Tabla 17 Impacto Residual

Impacto Residual

	D	I	C	A	T
[B]ACTIVOS ESENCIALES					
[E1] Información Confidencial	5	5	4		
[IS]SERVICIOS INTERNOS					
[is1] Voz sobre IP	2	2	2	2	
[is2] Internet	0	0	0		
[is4] Soporte al usuario	2	2	2		
[is3] servidor de nombres de dominio	4	4	4		
[SS] SERVICIOS SUBCONTRATADOS					
[ss1] impresión	2	4	2		
[ss2] alojamiento de servidor Web	4	4	4		
[ss3] Correo Electrónico	2	0	2		
[ss4] proveedor de servicio de internet	2	0	0		
[ss5] respaldo de datos	0	0	2		
[ss6] alojamiento de aplicaciones (hosting)	2	0	0		
[SW]APLICACIONES					
[sw1] Sistema Financiero CGWEB	4	3	3		
[sw2] Ofimática	2	3	2		
[sw3] servidor de directorio	4	4	4	3	
[sw4] sistema de gestión de base de datos (Oracle 11g)	6	3	4		
[sw5] sistema operativo (windows, linux)	2	3	3		
[sw6] hipervisor (gestor de la máquina virtual)	3		4		
[sw7]Sistema de Gestión Documental RUMIDOCS	2	3	3	3	
[sw8] Respaldos (acronis)	6	3	4		
[sw9]Antivirus (ESET)	4	3	3	3	
[sw10] Monitoreo de Red (PRTG)	2	3	2	3	
[sw11] Sophos SSL VPN Client	4	3	2	3	
[HW] EQUIPAMIENTO INFORMÁTICO					
[hw1]Servidores	5	5	5		
[hw2] Equipos Virtuales	5		2		
[hw3]Conmutador	2				
[hw4] punto de acceso inalambricos	4				
[hw5] teléfonos ip	2	5	4		
[hw6] informática personal (Computadores Todo en Uno, computador de escritorio, laptops)	3	2	2		
[hw7] Firewall	5	5	5		
[COM] REDES DE COMUNICACIONES					
[com1] red telefonica	3		5		
[com2] red de datos	3	3	3		
[com3] wifi	4		0		
[com4] red local	0	3	3	3	
[com5] red virtual	3	3	3		
[com6] VPN				2	
[SI] SOPORTES DE INFORMACIÓN					
[SI1]discos		0	2		
[SI2] memorias USB		4	4		
[SI3] material impreso		0	2		
[AUX] EQUIPAMIENTO AUXILIAR					
[aux1] Equipos de climatización	1				
[aux2] Fuentes de alimentación	1				
[aux3] cableado de datos (fibra y de alimentación)	4				
[aux4] sistema de alimentación interrumpida	1				
[aux5] sistema de video vigilancia	1				
[L]INSTALACIONES					
[i1] edificio	5				
[P]PERSONAL					
[p2]administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.	2	4	4		
[p1]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática	2	4	4		

Nota: Impacto Residual obtenido a partir del riesgo Current de PILAR Elaborado por: Autores en PILAR.

3.7. *Riesgo Residual*

El riesgo residual según (Consejo Superior de Administración Electrónica, 2012a), es la modificación del riesgo desde un valor potencial calculado anteriormente a un valor residual mediante la implementación de salvaguardas, PILAR calcula estos valores basándose en la valoración de las amenazas, la probabilidad y el nivel de madurez de las salvaguardas desplegadas que se puede ver en la Figura 19

Figura 21
Escala de Riesgo Residual.

Nota. Escala PILAR Riesgo Residual. Fuente: PILAR

La valoración del riesgo residual se puede ver en la Tabla 18 Riesgo Residualindica los valores obtenidos ya con las salvaguardas implementadas y utiliza la escala de la Figura 21

para medir que tan grave es el riesgo.

Tabla 18 Riesgo Residual

Riesgo Residual

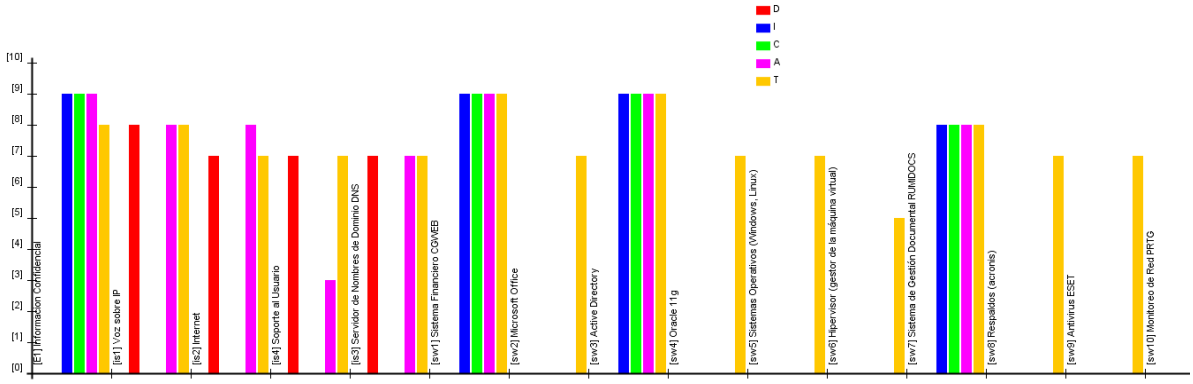
	D	I	C	A	T
[B]ACTIVOS ESENCIALES					
[E1] Información Confidencial	1,90	1,90	1,30		
[IS]SERVICIOS INTERNOS					
[is1] Voz sobre IP	2,10	2,10	2,10	0,79	
[is2] Internet	0,50	0,50	0,50		
[is4] Soporte al usuario	0,77	1,20	1,20		
[is3] servidor de nombres de dominio	1,80	2,30	2,30		
[SS] SERVICIOS SUBCONTRATADOS					
[ss1] impresión	2,10	2,70	2,10		
[ss2] alojamiento de servidor Web	2,00	1,80	1,80		
[ss3] Correo Electrónico	0,95	0,50	1,20		
[ss4] proveedor de servicio de internet	0,74	0,50	0,50		
[ss5] respaldo de datos	0,68	0,56	0,85		
[ss6] alojamiento de aplicaciones (hosting)	0,92	0,50	0,50		
[S]WAPLICACIONES					
[sw1] Sistema Fianciero CGWEB	2,10	1,40	1,40		
[sw2] Ofimática	0,97	1,70	1,40		
[sw3] servidor de directorio	1,80	1,80	1,90	0,94	
[sw4] sistema de gestión de base de datos (Oracle 11g)	2,90	1,70	1,80		
[sw5] sistema operativo (windows, linux)	0,97	1,70	1,80		
[sw6] hipervisor (gestor de la máquina virtual)	0,99	0,78	1,00		
[sw7]Sistema de Gestión Documental RUMIDOCS	1,00	1,70	1,80	0,94	
[sw8] Respaldos (acronis)	2,90	1,70	0,99		
[sw9]Antivirus (ESET)	2,10	1,80	1,80	0,94	
[sw10] Monitoreo de Red (PRTG)	0,97	1,80	0,98	0,94	
[sw11] Sophos SSL VPN Client	2,10	1,80	0,98	0,94	
[HW] EQUIPAMIENTO INFORMÁTICO					
[hw1]Servidores	2,60	1,70	1,70		
[hw2] Equipos Virtuales	3,50	0,71	0,71		
[hw3]Conmutador	1,00				
[hw4] punto de acceso inalambricos	2,10				
[hw5] teléfonos ip	1,00	2,60	2,10		
[hw6] informática personal (Computadores Todo en Uno, computador de escritorio, laptops)	1,40	0,81	1,10		
[hw7] Firewall	2,60	1,70	1,70		
[COM] REDES DE COMUNICACIONES					
[com1] red telefonica			3,10		
[com2] red de datos		0,95	0,95		
[com4] wifi			0,87		
[com5] red local		1,70	1,70	1,70	
[com6] red virtual		0,95	1,70		
[com3] VPN				0,84	
[SI] SOPORTES DE INFORMACIÓN					
[SI1]discos		0,50	1,40		
[SI2] memorias USB		0,50	1,40		
[SI3] material impreso		0,50	0,90		
[AUX] EQUIPAMIENTO AUXILIAR					
[aux1] Equipos de climatización	0,88				
[aux2] Fuentes de alimentación	0,88				
[aux3] cableado de datos (fibra y de alimentación)	0,94				
[aux4] sistema de alimentación interrumpida	0,70				
[aux5] sistema de video vigilancia	0,70				
[L]INSTALACIONES					
[i1] edificio	3,00				
[P]PERSONAL					
[p2]administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.	0,79	2,10	1,60		
[p1]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática	0,79	2,10	1,60		

Nota: Elaborado en PILAR a partir del riesgo Current dado por el programa. Elaborado por Autores en PILAR

3.8. *Informes*

Otra de las ventajas de utilizar la herramienta PILAR es que permite generar informes con gráficos referentes a las evaluaciones realizadas. La Figura 22 hace referencia a los valores de cada activo, esto con el fin de tener clara la situación en cuanto a las dimensiones que se ven afectadas en caso de que falle algún activo.

Figura 22
Gráfico Valor vs Activo



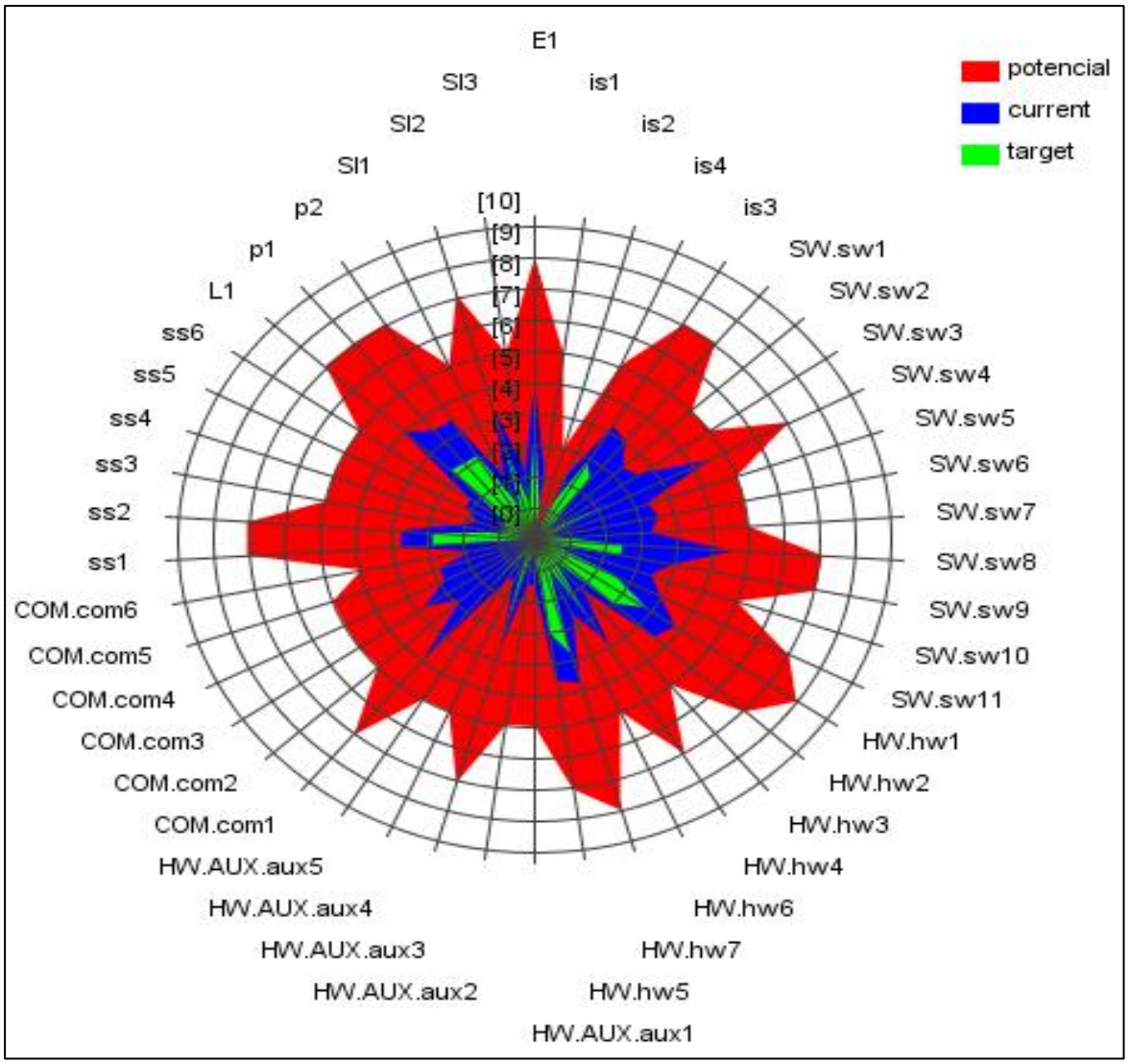
Nota. Gráfico comparativo del valor de los Activos. Fuente PILAR

En la

Figura 23 y

Figura 24 se ven reflejadas imágenes del impacto y riesgo acumulado respectivamente sobre los activos identificados, son gráficas radiales que permiten apreciar la diferencia al momento de implementar salvaguardas antes definidas logrando que disminuyan los valores en sus niveles de vulnerabilidad de los activos hasta llegar a un nivel objetivo.

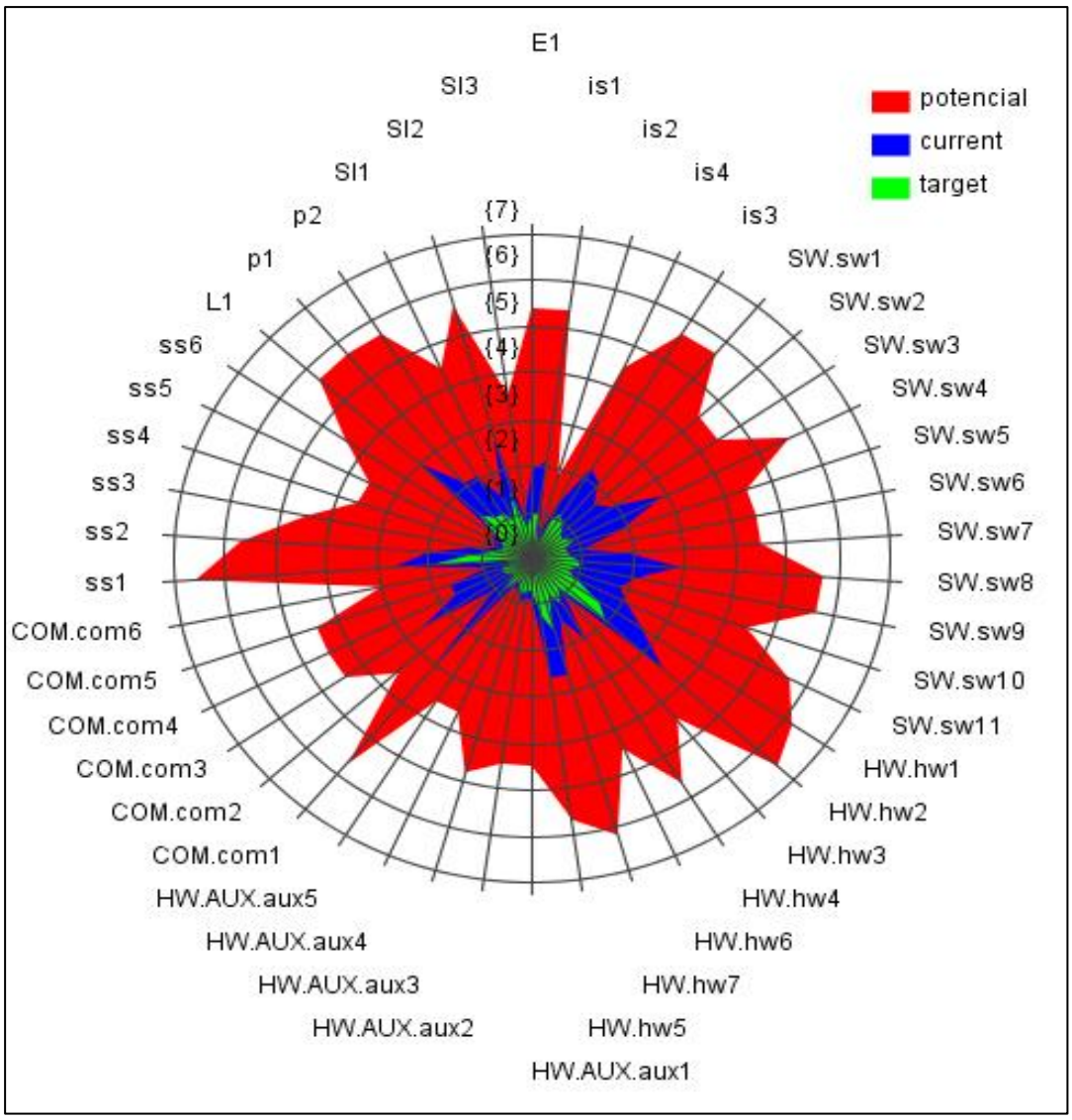
Figura 23
Gráfico Impacto Acumulado



Nota. Gráfico comparativo del Impacto Acumulado. Fuente PILAR

Figura 24

Gráfico Riesgo Acumulado



Nota. Gráfico comparativo Riesgo Acumulado. Fuente PILAR

CAPÍTULO 4

4. GESTIÓN DE RIESGOS

En esta etapa final, una vez realizado y concluido con el análisis de riesgos, es pertinente comunicar al personal de tecnología, acerca de los activos que han sido evaluados, indicando las amenazas encontradas y salvaguardas implementadas.

Cabe recordar que el presente análisis se ha enfocado en el estudio de los activos pertenecientes al departamento de tecnología, por tanto, el presente capítulo se subdivide en las siguientes actividades:

- Identificación de riesgos críticos.
- Tratamiento de riesgo a implementar.
- Plan de seguridad para controlar riesgos.

El objetivo de esta actividad es conocer aquellos activos que están expuestos a riesgos en un nivel mayor al permitido, esto con el objetivo de la implementación salvaguardas que impidan que las amenazas halladas se cristalicen.

4.1. *Identificación de riesgos críticos*

Por lo general en toda empresa sea esta pequeña, mediana o grande, los activos pertenecientes a la misma están expuestos a riesgos, ya sean estos depreciables, bajos medios, altos o críticos, por tanto, es necesario conocer los activos de mayor nivel de riesgo para que puedan ser tratados.

Luego de la evaluación dada a todos los activos identificados, se eligieron aquellos que poseen un nivel de riesgo medio y alto, detallados en la Tabla 19 obtenidos con la ayuda de la herramienta PILAR teniendo en cuenta los niveles de criticidad indicados en la

Figura 25 , identificación que sirve para realizar el tratamiento del riesgo.

Figura 25
Niveles de Criticidad Riesgos

Nota. Código de colores para identificar la Criticidad de Riesgos. Fuente PILAR

Tabla 19
Riesgos Críticos

Activo	Amenazas	Dimension	Valor	Valor Acumulado	Degradación	Impacto	Probabilidad	Riesgo
[hw1] Servidores	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	[9]	100%	[5]	0,043	2,60
	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[4]	0,051	2,30
	[N.1] Fuego	[D]	[9]	[9]	50%	[4]	0,051	2,30
	[N.2] Daños por agua	[D]	[9]	[9]	50%	[4]	0,051	2,30
[hw2] Equipos Virtuales	[E.24] Caída del sistema por agotamiento de recursos	[D]	[9]	[9]	50%	[5]	0,58	3,50
	[N.1] Fuego	[D]	[9]	[9]	50%	[4]	0,051	2,30
	[N.2] Daños por agua	[D]	[9]	[9]	50%	[4]	0,051	2,30
	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[4]	0,051	2,30
[hw4] Puntos de Acceso Inalambricos	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]		[9]	50%	[4]	0,044	2,10
[hw5] Telefonos IP	[E.15] Alteración de la información	[I]		[9]	50%	[5]	0,062	2,60
	[A.14] Interceptación de información (escucha)	[C]		[9]	50%	[4]	0,042	2,10
[hw7] Firewall	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	[9]	100%	[5]	0,043	2,60
	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[4]	0,051	2,30
	[N.2] Daños por agua	[D]	[9]	[9]	50%	[4]	0,051	2,30
	[N] Desastres naturales	[D]	[9]	[9]	50%	[4]	0,051	2,30
	[N.1] Fuego	[D]	[9]	[9]	50%	[4]	0,051	2,30
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[9]	[9]	50%	[4]	0,044	2,20
[is1] Voz sobre IP	[A.7] Uso no previsto	[I]		[9]	10%	[2]	0,62	2,10
	[A.7] Uso no previsto	[C]		[9]	10%	[2]	0,62	2,10
	[A.7] Uso no previsto	[D]	[8]	[9]	10%	[2]	0,62	2,10
[is3] Servidor de Nombres de Dominio DNS	[A.11] Acceso no autorizado	[C]		[9]	50%	[4]	0,056	2,30
	[E.2] Errores del administrador del sistema / de la seguridad	[C]		[9]	50%	[4]	0,056	2,30
	[A.11] Acceso no autorizado	[I]		[9]	50%	[4]	0,056	2,30
	[E.2] Errores del administrador del sistema / de la seguridad	[I]		[9]	50%	[4]	0,056	2,30

	[sw1] Sistema Financiero CGWEB	[I.5] Avería de origen físico o lógico	[D]		[9]	50%	[4]	0,046	2,10
	[sw4] Oracle 11g	[E.18] Destrucción de la información	[D]		[9]	50%	[6]	0,035	2,90
	[sw8] Respaldos (acronis)	[E.18] Destrucción de la información	[D]		[9]	50%	[6]	0,035	2,90
		[A.18] Destrucción de la información	[D]		[9]	50%	[6]	0,035	2,90
		[I.5] Avería de origen físico o lógico	[D]		[9]	50%	[4]	0,046	2,10
	[sw9] Antivirus ESET	[I.5] Avería de origen físico o lógico	[D]		[9]	50%	[4]	0,045	2,10
	[sw11] Sophos SSL VPN Client	[I.5] Avería de origen físico o lógico	[D]		[9]	50%	[4]	0,045	2,10
	[com1] Red telefónica	[A.14] Interceptación de información (escucha)	[C]		[9]	50%	[5]	0,114	3,10
	[com3] Wifi	[I.8] Fallo de servicios de comunicaciones	[D]		[9]	10%	[4]	0,22	2,60
	[ss1] Servicio de Impresión	[A.5] Suplantación de la identidad	[I]		[9]	50%	[4]	0,32	2,70
		[A.7] Uso no previsto	[I]		[9]	10%	[2]	0,62	2,10
		[A.7] Uso no previsto	[C]		[9]	10%	[2]	0,62	2,10
		[A.7] Uso no previsto	[D]	[7]	[9]	10%	[2]	0,62	2,10
	[ss2] Alojamiento de servidor Web	[E.18] Destrucción de la información	[D]	[7]	[9]	50%	[4]	0,05	2,00
	[L1] Edificio	[N.*.1] Tormentas	[D]	[8]	[9]	50%	[5]	0,09	3,00
		[N.2] Daños por agua	[D]	[8]	[9]	50%	[5]	0,09	3,00
		[N.1] Fuego	[D]	[8]	[9]	50%	[5]	0,089	3,00
	[p1] Sr. Ismael Aldaz – Técnico en Informática	[E.4] Errores de configuración	[I]		[9]	50%	[4]	0,039	2,10
	[p2] Ing. Luis Villalta - Jefe de TIC´s.	[E.4] Errores de configuración	[I]		[9]	50%	[4]	0,039	2,10
	[SI2] Memorias USB	[E.19] Fugas de información	[C]	[7]	[9]	50%	[4]	0,12	2,70

Nota. Tabla resumen de los riesgos críticos encontrados luego de finalizado el análisis. Elaborado por Autores basado en resultados de PILAR.

En la tabla también se muestra de manera resumida los resultados del análisis de riesgos, están los activos críticos, las amenazas con la dimensión afectada, el valor del activo, la degradación, el impacto y la probabilidad. Todos estos datos influyen para el cálculo del riesgo final y ayudan a entender el por qué estos riesgos son críticos.

Para la identificación de los activos con riesgos más críticos se utilizó la herramienta PILAR, con esta herramienta se identificó aquellos activos que tienen un riesgo medio-alto, es decir aquellos activos que se encuentran en un nivel de criticidad mayor o igual que 2 y menor que 4, según lo indica la leyenda de niveles de criticidad.

De igual forma en la selección de los activos más críticos se consideró la amenaza que afecta a cada activo y el nivel de degradación que puede verse afectado.

4.2. *Tratamiento de riesgo a implementar*

Luego de identificar los activos con riesgos más críticos, se procede a la gestión del tratamiento de riesgos, mismo que consiste en la modificación del riesgo mediante medidas adecuadas implantadas.

Las estrategias sugeridas por MAGERIT para gestionar el tratamiento de riesgos están representadas en la Tabla 20.

Tabla 20.
Estrategias para el tratamiento de Riesgos

Estrategias	Definición
Evitar o eliminar el riesgo	Eliminar activos para que desaparezca el riesgo. (Probabilidad de ocurrencia con Impacto Muy Alto)
Reducir o mitigar el riesgo	Implementar acciones para reducir amenaza.
Transferir o compartir el riesgo	Transferir el inconveniente a terceros (proveedores).
Aceptar el riesgo	La organización no tiene otra opción por tanto acepta el riesgo, aprende a convivir con él. (Probabilidad Muy Baja de Ocurrencia)

Nota. Estrategias que se usaran para el tratamiento de riesgos. Elaborado por: Los autores, a través del Libro I Magerit-versión 3.0 página 49.

Para realizar la gestión del tratamiento del riesgo, se indicó que las dos estrategias a emplearse son aceptar o mitigar el riesgo, debido a que son acciones que están dentro del alcance del departamento, las otras estrategias como son eliminar y transferir no se consideran debido al factor económico.

Tabla 21
Probabilidad de Ocurrencia

CS	CASI SEGURO
MA	MUY ALTO
P	POSIBLE
PP	POCO PROBABLE
MB	SIGLOS
MR	MUY RARA
0	

Nota. Valores que se darán para valorar la probabilidad de ocurrencia. Fuente: PILAR

Figura 26
Niveles de Criticidad de Riesgo

Fuente PILAR

Un ejemplo de las estrategias utilizadas para tratar el riesgo de un activo se puede evidenciar en la ¡Error! La autoreferencia al marcador no es válida. **teniendo en cuenta los valores de la**

Tabla 21 , los niveles de criticidad de riesgo de la Figura 26

y el tratamiento de riesgo a implementar como se indica en Tabla 20.

Tabla 22
Tratamiento de Riesgo VoIP

ACTIVO	AMENAZA	DIMENSIÓN	RIESGO	CRITICIDAD	PROBABILIDAD	TRATAMIENTO
[is1] Voz sobre IP	[A.7] Uso no previsto	C	2,1	Medio	P	Mitigar
	[A.7] Uso no previsto	D	2,1	Medio	P	
	[A.7] Uso no previsto	I	2,1	Medio	P	

Nota. Descripción del tratamiento de riesgo que se va a realizar por cada amenaza en VoIP

Elaborado por Autores

El tratamiento de riesgo completo por cada activo crítico identificado se encuentra en el **ANEXO F TRATAMIENTO DE RIESGOS**

4.3. *Plan de seguridad para controlar los riesgos*

Para la etapa final es primordial socializar con el personal implicado en las distintas áreas que intervienen acerca de los activos que han sido considerados para la evaluación juntamente con sus amenazas y respectivas salvaguardas.

Es necesario considerar un plan de seguridad para controlar los riesgos y es pertinente establecer los pasos o procesos necesarios con el fin de evitar o mitigar la materialización de incidentes que puedan provocar la afectación de la continuidad normal de las operaciones de los servicios indispensables en la organización.

Para esta actividad se detallarán en un plan de ejecución las medidas técnicas a tomar en cuenta para la solución de posibles inconvenientes.

4.3.1. Marco Referencial

Se propone una política de seguridad en el **ANEXO B POLÍTICA DE SEGURIDAD**, en la que se describen parámetros y personas responsables que intervienen para mejorar la seguridad

informática de la empresa. La mencionada política debe ser revisada por la jefatura de tecnología y aprobada por la Gerencia de Planificación y Gestión Empresarial, para realizar correcciones o mejoras con el fin de implementarla.

4.3.2. Plan de ejecución

En este apartado se detallan los pasos a seguir con el objetivo de reanudar de manera oportuna los servicios frente a los riesgos que han sido identificados y que a continuación se detallan:

4.3.2.1. Riesgo: [A.5] Suplantación de la identidad del usuario.

Activos afectados: [ss] Servicios Subcontratados.

Personal Involucrado: Personal TI, Personal de Talento Humano, usuarios finales.

Periodicidad: Informes finales mensualmente, capacitaciones semestrales.

Medidas Técnicas:

- Proporcionar a los usuarios métodos y recomendaciones, por ejemplo para protegerse contra la suplantación de identidad, emplear contraseñas seguras y únicas para cada usuario, otras sugerencias constan en el **ANEXO B POLÍTICA DE SEGURIDAD**.
- Establecer una contraseña para impedir el acceso al panel de administración del equipo de impresión a usuarios no autorizados.
- Adquirir un software de conteo de impresiones y copiado para llevar un registro mensual del número de impresiones y copiado por usuario, con el fin de confirmar si realmente es el número de transacciones indicadas por el proveedor.
- El departamento de tecnología deberá realizar capacitaciones al menos una vez por año acerca del buen uso del servicio y mediante campañas de educación promover el ahorro de impresiones y de papel.

- El personal de tecnología deberá enviar los informes a la Gerencia de Planificación y Gestión Empresarial con el total de impresiones y copiado sin exponer las contraseñas de acceso al servicio de los usuarios con el fin de que estas no se divulguen.
- Capacitar al personal mediante charlas de al menos una vez por año para que por ningún motivo proporcionen contraseñas personales para la utilización del servicio, de igual manera que se realice el cierre de sesión al momento de haber terminado de realizar la actividad.

4.3.2.2. Riesgo: [A.7] Uso no previsto.

Activos afectados: [is] Servicios Internos.

Personal Involucrado: Personal TI, usuarios finales.

Periodicidad: Control y monitoreo diario de los servicios, revisión de configuraciones mensual.

Medidas Técnicas:

- Definir contraseñas únicas y proporcionarlas a cada usuario para hacer uso del servicio de telefonía hacia fuera del perímetro empresarial.
- Los usuarios deberán hacer uso de los servicios informáticos de forma responsable, haciendo conciencia y salvaguardando los recursos necesarios con el fin de evitar hacer usos no previstos, el departamento de tecnología será el responsable de la capacitación de la utilización adecuada de los servicios brindados para garantizar la continuidad de estos.
- En el servicio de telefonía, segmentar el destino de las llamadas telefónicas por usuario en la configuración SIP del servicio de telefonía, con el objetivo de que el servicio sea utilizado únicamente para los fines necesarios.

- Los funcionarios que hagan uso de los servicios informáticos serán los responsables directos sobre las acciones que realicen sobre estos, así como el manejo del usuario y contraseña que han sido proporcionados para su respectivo acceso.
- Solicitar el compromiso por parte de los usuarios a tener sus contraseñas personales reservadas sin proporcionarlas a nadie y de ser posible el caso firmar una declaración **(ANEXO A. DECLARACIÓN PERSONAL DE CONFIDENCIALIDAD Y PRIVACIDAD DE CONTRASEÑAS)** en la que se comprometen a realizarlo.

4.3.2.3. Riesgo: [A.11] Acceso no autorizado.

Activos afectados: [is] Servicios Internos.

Personal Involucrado: Personal de TI.

Periodicidad: Seguimiento diario de la utilización de servicios

Medidas Técnicas:

- Establecer el número de intentos que puede realizar un usuario al momento de introducir usuario y contraseña incorrecta, en el directorio activo de hasta máximo 3 intentos.
- Configurar el acceso al sistema para la suspensión de la sesión automática a la que se accede si es que esta no se encuentra en uso.
- Las contraseñas que tiene privilegios de administradores deben ser únicas en comparación a las contraseñas de usuario y por ningún motivo deberán ser proporcionadas a personas ajenas.
- El departamento de tecnología mediante la implementación de grupos de usuarios deberá organizar los privilegios de los usuarios en cuanto a la seguridad.
- Las contraseñas proporcionadas para el acceso a los servicios internos deben estar controladas y administradas por el departamento de tecnología.

- Por ningún motivo se deberán compartir contraseñas de acceso ni usuarios al resto de personal administrativo, estas deben ser tratadas con confidencialidad.
- En el caso de existir cambio de contraseñas administradoras, por ningún motivo deben ser revelados por medios de comunicación electrónica, sean estos mails o chats.
- Omitir dialogar acerca de credenciales de acceso a los servicios internos enfrente de otros usuarios.
- El departamento de tecnología es responsable de la administración de los servicios internos, por tanto, es quien velará por la correcta funcionalidad de estos y serán responsables de las acciones realizadas.

4.3.2.4. Riesgo: [A.14] Interceptación de información (escucha).

Activos afectados: [hw] Hardware, [com] Comunicaciones.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Revisión de configuración mensual de los equipos.

Medidas Técnicas:

- Realizar las configuraciones necesarias en los equipos de comunicación para garantizar que la información no se desvíe y llegue al destino indicado para evitar errores de intercepción de la información y de re-encaminamiento.
- Realizar la encriptación de las llamadas que puedan considerarse como críticas.
- Evitar hablar por telefonía IP de temas de vital importancia frente a personas que puedan tener acceso a esa información para evitar su divulgación.
- Los funcionarios son los responsables de la información que manejan, al existir información de vital importancia lo recomendable es tratar estos asuntos mediante reuniones presenciales para mantener la información de forma confidencial.

4.3.2.5. Riesgo: [A.18] Destrucción de información.

Activos afectados: [ss] Servicios Subcontratados, [sw] Software.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Monitoreo diaria de utilización de servicios, verificación diaria del correcto funcionamiento de copias de seguridad.

Medidas Técnicas:

- Verificar el registro de logs en los sistemas al menos una vez por semana para tener un registro de los usuarios que han realizado alguna acción que pueda afectar a la continuidad de los servicios.
- Supervisar el acceso a la información cuando un funcionario la solicite mediante la asignación de perfiles de seguridad previa autorización de la máxima autoridad o jefe inmediato.
- Gestionar el almacenamiento de copias de información en la nube y monitorizar el cumplimiento de estos, en caso de no realizarse la copia verificar el inconveniente y proceder a realizarla de forma manual.
- Gestionar un plan de respaldos oportuno para estaciones de trabajo y servidores que garanticen la integridad de la información tal y como se indica en el **ANEXO B POLÍTICA DE SEGURIDAD (RESPALDO DE LA INFORMACIÓN).**
- El departamento de tecnología es el encargado de proteger la integridad y garantizar la disponibilidad de la información, se debe establecer un procedimiento para recuperación de la información o respaldo de la misma.
- Los funcionarios son los responsables del acceso a la información mediante los perfiles de seguridad que se les otorga, el administrar los recursos informáticos es responsabilidad de cada usuario, así como el de velar por la integridad de la información.

[E] Errores y fallos no intencionados.

4.3.2.6. Riesgo: [E.2] Errores del administrador del sistema / de la seguridad.

Activos afectados: [is] Servicios Internos.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Revisión de configuración de equipos mensual, respaldo de configuración previo cambio.

Medidas Técnicas:

- Para los errores de configuración gestionar un plan de backups previa a cualquier configuración de equipos que debe ser puesto a prueba con anterioridad para solucionar problemas de administración y configuración.
- El departamento de tecnología deberá asegurar que los sistemas y/o servicios que se alojen en los servidores tengan la capacidad de generar logs que serán monitoreados paulatinamente con el fin de evitar que se afecte a la disponibilidad e integridad de estos.
- Monitoreo constante de servicios, estado de la red, y otros recursos informáticos mediante aplicaciones que permitan garantizar la funcionalidad correcta de la infraestructura tecnológica.
- El departamento de tecnología debe de registrar en manuales los procedimientos de configuraciones de servidores u otros equipos informáticos que son administrados por ellos.
- Implementar una bitácora con los registros de las incidencias más comunes presentadas y las soluciones oportunas que se les pueda emplear.
- Brindar capacitaciones constantes al personal de tecnología con el fin de mantener una actualización adecuada y correcta administración de los sistemas con el fin de permitir

la implementación de nuevas tecnologías que ayuden a mejorar la seguridad informática.

4.3.2.7. Riesgo: [E.4] Errores de configuración.

Activos afectados: [D.conf] datos de configuración.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Cada 2 semanas o cuando se realice una configuración.

Medidas Técnicas:

- Realizar copias de configuración de los equipos informáticos, con el fin de emplearlos en algún momento necesario.
- Comprobar que los backup de las configuraciones realizadas funcionen de manera correcta y garantizar la disponibilidad de los equipos.
- Establecer como buena práctica el realizar pruebas de configuración tanto en servidores, equipos de cómputo y equipos de comunicación, previo a su configuración final.
- El departamento de tecnología debe de contar con manuales de configuración de servidores u otros equipos informáticos que son administrados por ellos.
- Gestionar una bitácora de incidentes que permitan ser identificados de mejor manera y tratados con la solución óptima documentada.
- Brindar capacitaciones constantes al departamento de sistemas acerca de la correcta configuración de equipos informáticos, compatibilidad de aplicaciones que permitan respuestas óptimas a posibles incidentes.

4.3.2.8. Riesgo: [E.15] Alteración de la información.

Activos afectados: [hw] Hardware.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Verificación del estado de los equipos semanalmente.

Medidas Técnicas:

- Controlar el acceso a la configuración de equipos informáticos, mediante claves de seguridad robustas y el acceso al hardware mediante candados o sellos de seguridad.
- Monitorear el funcionamiento de los equipos y las alteraciones que pudieron haberse realizado, mediante la implementación de un software que monitoree cambios tanto en hardware como en software.
- El departamento de tecnología debe de contar con backup de la configuración e información del equipamiento informático.
- El departamento de tecnología debe tener manuales de configuración de los equipos en caso de alteración accidental de la información.
- El funcionario es el responsable de la protección del equipo informático, por tanto, debe evitar la manipulación del equipo y solicitar asistencia técnica en caso de requerirla.

4.3.2.9. Riesgo: [E.18] Destrucción de información.

Activos afectados: [sw] Software.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Cada 2 semanas o cuando se realice una configuración.

Medidas Técnicas:

- Establecer las responsabilidades acerca del manejo de la información.
- Gestionar un plan de respaldos oportuno para estaciones de trabajo y servidores que permitan recuperar la información en caso de pérdida como se indica en el **ANEXO B POLÍTICA DE SEGURIDAD.**

- El departamento de tecnología es el encargado de proteger la integridad y garantizar la disponibilidad de la información, deberá establecer un proceso para la recuperación de la información o respaldo.
- El funcionario es el responsable del acceso que se le otorga, el administrar los recursos informáticos es responsabilidad de cada usuario, así como el de velar por la integridad de la información.

4.3.2.10. Riesgo: [E.19] Fugas de información.

Activos afectados: [SI] Soporte de Información.

Personal Involucrado: Personal de TI, talento humano, usuarios finales.

Periodicidad: Revisar cambios u alteraciones de hardware o software semanalmente.

Medidas Técnicas:

- Considerar el bloqueo de puertos USB en los equipos de cómputo para evitar que los funcionarios conecten dispositivos USB sin permiso o supervisión con el fin de contrarrestar la fuga de información.
- El departamento de tecnología es el encargado de proteger la integridad y garantizar la disponibilidad de la información, considerar la no utilización de dispositivos USB u otros dispositivos de almacenamiento externo para el transporte de la información.
- Gestionar el compromiso por parte de los usuarios en conjunto con el departamento de Talento Humano para mantener la información confidencial para la organización y de ser posible firmar un acuerdo de confidencialidad.

4.3.2.11. Riesgo: [E.23] Errores de mantenimiento / actualizaciones.

Activos afectados: [hw] Hardware.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Respaldos cada mes, mantenimiento preventivo y/o correctivo del equipamiento informático por lo menos 2 veces por año en condiciones normales.

Medidas Técnicas:

- Realizar respaldos periódicos de configuración del equipo por lo menos una vez al mes.
- Considerar el mantenimiento preventivo y/o correctivo del equipamiento informático por lo menos 2 veces por año.
- Verificar si las actualizaciones de software en los equipos son pertinentes o tienen incidencia directa en cuanto a la compatibilidad de las aplicaciones.
- El departamento de tecnología deberá documentar y monitorear el funcionamiento y estado del equipo, al considerarse como fundamental en la continuación de los servicios.
- Establecer un cronograma de mantenimientos preventivos y correctivos para garantizar la continuidad de los equipos, gestionar el proceso de garantía de equipos informáticos que aún cumplan con esta característica.

4.3.2.12. Riesgo: [E.24] Caída del sistema por agotamiento de recursos.

Activos afectados: [hw] Hardware.

Personal Involucrado: Personal de TI.

Periodicidad: Monitoreo de recursos mensual.

Medidas Técnicas:

- Considerar el mantenimiento preventivo y/o correctivo de los servidores por lo menos dos veces por año.
- Realizar copias de seguridad de forma regular, tanto de configuración como de información.

- Realizar el monitoreo de recursos de los servidores con el fin de verificar la disponibilidad de espacio en disco o memoria RAM.
- Registrar en una bitácora o matriz los recursos existentes en los servidores y documentar las incidencias que puedan presentarse en los equipos mediante el análisis de logs que pueda presentar el visor de registros.
- El personal de tecnología es el encargado de verificar el correcto funcionamiento de los equipos informáticos y tomar las decisiones pertinentes para prevenir caídas de sistemas o servicios.
- El personal de tecnología es el responsable de la verificación y administración de los recursos que emplean los equipos informáticos para garantizar su normal desempeño, en caso de necesitar mejorar el rendimiento, se deberá realizar la gestión de adquisición de componentes que permitan optimizar su funcionamiento.

Seguridad [I] de Origen Industrial

4.3.2.13. Riesgo: [I.5] Avería de origen físico o lógico.

Activos afectados: [sw] Software, [hw] Hardware.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Revisión del estado de los equipos mensual, compra de partes y piezas semestral.

Medidas Técnicas:

- Realizar seguimiento a los contratos de compra de equipos informáticos con el fin de verificar el tiempo de garantía y en general que se obtiene de dicha garantía, en caso de ya no existir vigencia tecnológica de los equipos informáticos considerarlos dentro de un plan para realizar mantenimientos preventivos y/o correctivos.

- Realizar un control de los recursos existentes en los equipos virtuales con el objetivo de garantizar la operatividad de los mismos, hacer énfasis en memoria y espacio en disco.
- Gestionar el buen uso de los equipos informáticos con los usuarios mediante la capacitación del manejo y cuidado de equipos por lo menos una vez al año, para alargar el tiempo de vida del equipamiento.
- Ejecutar la compra de piezas o repuestos para los equipos informáticos y mantener un stock que permita el reemplazo de estos en caso de avería o daño de algún equipo, con el objetivo de disminuir el tiempo de inoperatividad que pueda causar la ausencia de estas partes o piezas.
- Capacitar al personal por lo menos una vez por año acerca del uso tanto de los equipos informáticos como de aplicaciones con el fin de minimizar errores por parte de los usuarios en el manejo de aplicaciones o utilización de equipos.

4.3.2.14. Riesgo: [I.7] Condiciones inadecuadas de temperatura o humedad.

Activos afectados: [hw] Hardware.

Personal Involucrado: Personal de TI.

Periodicidad: Verificación del estado de temperatura y humedad de los cuartos de datos a diario.

Medidas Técnicas:

- Implementar controles de temperatura en todos los cuartos de datos que tengan equipos informáticos y de comunicaciones, para la verificación de humedad y temperatura adecuada en cada cuarto.

- Considerar la reubicación de los equipos como Access point o switch de acceso, esto debido a las condiciones de temperatura que provoca el tipo de material de la construcción de las instalaciones.
- Gestionar el respaldo de ventilación o aire acondicionado en el centro de datos con el propósito de que si falla el primario entre en ejecución el aire de respaldo.
- El departamento de tecnología es el responsable del correcto funcionamiento de los equipos, por tanto, se recomienda como buena práctica verificar el estado y las condiciones en las que se encuentran cada uno de los equipos al iniciar el día.

4.3.2.15. Riesgo: [I.8] Fallo de servicios de comunicaciones.

Activos afectados: [com] Comunicaciones.

Personal Involucrado: Personal de TI, usuarios finales.

Periodicidad: Verificación de las instalaciones y estado de las conexiones mensual.

Medidas Técnicas:

- Controlar el acceso al centro de datos para asegurar el perímetro de los equipos de comunicaciones y servidores, considerar una bitácora de visitas para controlar el ingreso de personas extrañas.
- Eliminar conexiones intermedias que impidan un cableado directo entre los equipos de comunicación y los puntos de red, considerar el diseño de punto a punto.
- Verificar la ubicación y cableado de los equipos los cuales no deben estar expuestos al personal para evitar desconexiones tanto eléctricas como de datos, en caso de ser necesario la implementar de canaletas que proteja el cableado.

- Asegurarse de que los equipos estén bien resguardados ya sea con cerraduras en los racks o un sistema de control de acceso digital con el que se evite la manipulación de personas no autorizadas en el cuarto de datos.
- Capacitación al personal de tecnología por lo menos dos veces por año, para realizar las configuraciones pertinentes y garantizar la continuidad de los servicios de comunicaciones, evitar el exceso de confianza al momento de realizar dichas configuraciones.

Seguridad [N] Desastres Naturales

4.3.2.16. Riesgo: [N.] Desastres Naturales-Tormentas.*

Activos afectados: [hw] Hardware.

Personal Involucrado: Personal de TI, personal de salud ocupacional, personal de mantenimiento, usuarios finales.

Periodicidad: Copias de seguridad de los equipos mensual, limpieza de ductos y cajas de desfogue mensual.

Medidas Técnicas:

- Considerar respaldos de equipos en otras instalaciones, bien sea el caso fuera de la empresa, implementación o configuración de servidores espejo o almacenamiento en la nube, con el propósito de realizar un plan de recuperación de los servicios más críticos y gestionar el respaldo de la información.
- Realizar backups de configuración de equipos periódicamente, se recomienda respaldar esta información mínimo una vez por mes.
- Establecer un plan de evacuación de equipos más críticos con el fin de preservar estos activos.

- Coordinar con el departamento de seguridad ocupacional y ambiental el proceso a seguir en caso de sismo o terremoto, de igual manera las vías de evacuación y zonas definidas como seguras dentro del perímetro empresarial para el personal.
- Coordinar con el área de mantenimiento la limpieza de cajas de desfogue de agua para evitar la acumulación de lodo y hierba que afecten al cableado eléctrico y de datos.
- Capacitación al personal por lo menos dos veces por año de cómo debe actuar en caso de sismos o terremotos, esto en conjunto con el departamento de seguridad ocupacional y ambiental.

4.3.2.17. Riesgo: [N1] Fuego.

Activos afectados: [hw] Hardware, [i] Edificio.

Personal Involucrado: Personal de TI, personal de salud ocupacional, personal de mantenimiento, usuarios finales.

Periodicidad: Capacitaciones semestrales, verificación del estado de las instalaciones mensual.

Medidas Técnicas:

- Implementación alarmas y sistemas de detección de fuego en los centros de datos, de igual manera la colocación de extintores a base de dióxido de carbono o de agua pulverizada en lo posible junto a la puerta de ingreso del cuarto de datos.
- Considerar un plan de evacuación de equipos informáticos más críticos con el fin de preservar estos activos.
- Realizar mantenimiento eléctrico de los tableros de energía por lo menos 2 veces al año en conjunto con el departamento de mantenimiento para evitar cortos circuitos y sobrecargas de electricidad.

- En caso de existir humo o fuego dentro de las instalaciones tomar acciones pertinentes como comunicar a los entes de emergencia como policía o bomberos.
- Coordinar con el departamento de seguridad ocupacional y ambiental el proceso a seguir en caso de incendio, de igual manera las vías de evacuación y zonas definidas como seguras dentro del perímetro empresarial para el personal.
- Capacitación al personal por lo menos 2 veces al año de cómo debe actuar en caso de incendios, esto en conjunto con el departamento de seguridad ocupacional y ambiental.

4.3.2.18. Riesgo: [N.2] Daños por agua.

Activos afectados: [hw] Hardware, [i] Edificio.

Personal Involucrado: Personal de TI, personal de salud ocupacional, personal de mantenimiento, usuarios finales.

Periodicidad: Capacitaciones semestrales, verificación del estado de las instalaciones mensual.

Medidas de Técnicas:

- Al encontrarse las instalaciones en una zona cercana a ríos pueden ocurrir incidentes de inundaciones, para ello es de vital importancia considerar la limpieza de desfogues que permitan que el agua no se acumule y provoque daños en los equipos.
- Considerar un plan de evacuación de equipos más críticos con el fin de preservar estos activos.
- En caso de existir acumulación de agua dentro de las instalaciones tomar acciones pertinentes como comunicar a los entes de emergencia como policía o bomberos.
- Coordinar con el departamento de mantenimiento la limpieza de drenajes o desfogues de agua en las instalaciones por lo menos una vez al año.

- Coordinar con el departamento de seguridad ocupacional y ambiental el proceso a seguir en caso de inundación, de igual manera las vías de evacuación y zonas definidas como seguras dentro del perímetro empresarial para el personal.
- Capacitación al personal por lo menos dos veces al año de cómo debe actuar en caso de inundación, esto en conjunto con el departamento de seguridad ocupacional y ambiental.

Luego de definir los procedimientos a seguir conforme al plan de seguridad, no se ha considerado tiempo para el plan de ejecución debido a que depende de muchos factores tanto administrativos como económicos, de igual manera se pone a consideración para revisión y aprobación de la máxima autoridad o directorio.

Luego de terminar con el estudio de la asignación de salvaguardas existentes en el riesgo actual o Current, la implementación de salvaguardas al nivel de riesgo target u objetivo, los riesgos y su impacto disminuyen de forma considerable, únicamente en los activos de Servicio de Impresión y Equipos virtuales se tiene la reducción de un riesgo alto a un riesgo medio tal y como se indica en la .

Tabla 23 .

Tabla 23

Resultados del tratamiento de riesgo

Activo	Amenazas	Dimensión	Valor	Valor Acumulado	Degradación	Impacto	Probabilidad	Riesgo
[hw1] Servidores	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	[9]	100%	[4]	MR	1,6
	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[3]	MR	1,2
	[N.1] Fuego	[D]	[9]	[9]	50%	[3]	MR	1,2
	[N.2] Daños por agua	[D]	[9]	[9]	50%	[3]	MR	1,2
[hw2] Equipos Virtuales	[E.24] Caída del sistema por agotamiento de recursos	[D]	[9]	[9]	50%	[3]	PP	2,00
	[N.1] Fuego	[D]	[9]	[9]	50%	[3]	MR	1,2
	[N.2] Daños por agua	[D]	[9]	[9]	50%	[3]	MR	1,2
	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[3]	MR	1,2
[hw4] Puntos de Acceso Inalambricos	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]		[9]	50%	[3]	MR	1,1
[hw5] Telefonos IP	[E.15] Alteración de la información	[I]		[9]	50%	[3]	MR	1,2
	[A.14] Interceptación de información (escucha)	[C]		[9]	50%	[3]	MR	1,2
[hw7] Firewall	[I.7] Condiciones inadecuadas de temperatura o humedad	[D]	[9]	[9]	100%	[4]	MR	1,6
	[I.5] Avería de origen físico o lógico	[D]	[9]	[9]	50%	[3]	MR	1,2
	[N.2] Daños por agua	[D]	[9]	[9]	50%	[3]	MR	1,2
	[N] Desastres naturales	[D]	[9]	[9]	50%	[3]	MR	1,2
	[N.1] Fuego	[D]	[9]	[9]	50%	[3]	MR	1,2
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[D]	[9]	[9]	50%	[3]	MR	1,2

	[is1] Voz sobre IP	[A.7] Uso no previsto	[I]		[9]	10%	[1]	PP	0,99
		[A.7] Uso no previsto	[C]		[9]	10%	[1]	PP	0,99
		[A.7] Uso no previsto	[D]	[8]	[9]	10%	[1]	PP	0,99
	[is3] Servidor de Nombres de Dominio DNS	[A.11] Acceso no autorizado	[C]		[9]	50%	[2]	MR	0,92
		[E.2] Errores del administrador del sistema / de la seguridad	[D]	[7]	[9]	50%	[3]	MR	1,1
		[A.11] Acceso no autorizado	[I]		[9]	50%	[2]	MR	0,92
		[E.2] Errores del administrador del sistema / de la seguridad	[I]		[9]	50%	[2]	MR	0,92
	[sw1] Sistema Financiero CGWEB	[I.5] Avería de origen físico o lógico	[D]		[9]	50%	[2]	MR	0,95
	[sw4] Oracle 11g	[E.18] Destrucción de la información	[D]		[9]	50%	[2]	MR	0,94
	[sw8] Respaldos (acronis)	[E.18] Destrucción de la información	[D]		[9]	50%	[2]	MR	0,94
		[A.18] Destrucción de la información	[D]		[9]	50%	[2]	MR	0,94
		[I.5] Avería de origen físico o lógico	[D]		[9]	50%	[2]	MR	0,95
	[sw9] Antivirus ESET	[I.5] Avería de origen físico o lógico	[D]		[9]	50%	[2]	MR	0,95
	[sw11] Sophos SSL VPN Client	[I.5] Avería de origen físico o lógico	[D]		[9]	50%	[2]	MR	0,95
	[com1] Red telefónica	[A.14] Interceptación de información (escucha)	[C]		[9]	50%	[2]	PP	0,94
	[com3] Wifi	[I.8] Fallo de servicios de comunicaciones	[D]		[9]	10%	[0]	MR	0,58
	[ss1] Servicio de Impresión	[A.5] Suplantación de la identidad	[I]		[9]	50%	[3]	PP	2,00
		[A.7] Uso no previsto	[I]		[9]	10%	[1]	PP	0,99
		[A.7] Uso no previsto	[C]		[9]	10%	[1]	PP	0,99
		[A.7] Uso no previsto	[D]	[7]	[9]	10%	[1]	PP	0,99
	[ss2] Alojamiento de servidor Web	[E.18] Destrucción de la información	[D]	[7]	[9]	50%	[3]	MR	1,1
	[L1] Edificio	[N.*.1] Tormentas	[D]	[8]	[9]	50%	[3]	MR	1,4
		[N.2] Daños por agua	[D]	[8]	[9]	50%	[3]	MR	1,4
		[N.1] Fuego	[D]	[8]	[9]	50%	[3]	MR	1,4
	[p1] Sr. Ismael Aldaz – Técnico en Informática	[E.4] Errores de configuración	[I]		[9]	50%	[3]	MR	1,1
	[p2] Ing. Luis Villalta - Jefe de TIC´s.	[E.4] Errores de configuración	[I]		[9]	50%	[3]	MR	1,1
	[SI2] Memorias USB	[E.19] Fugas de información	[C]	[7]	[9]	50%	[3]	PP	1,5

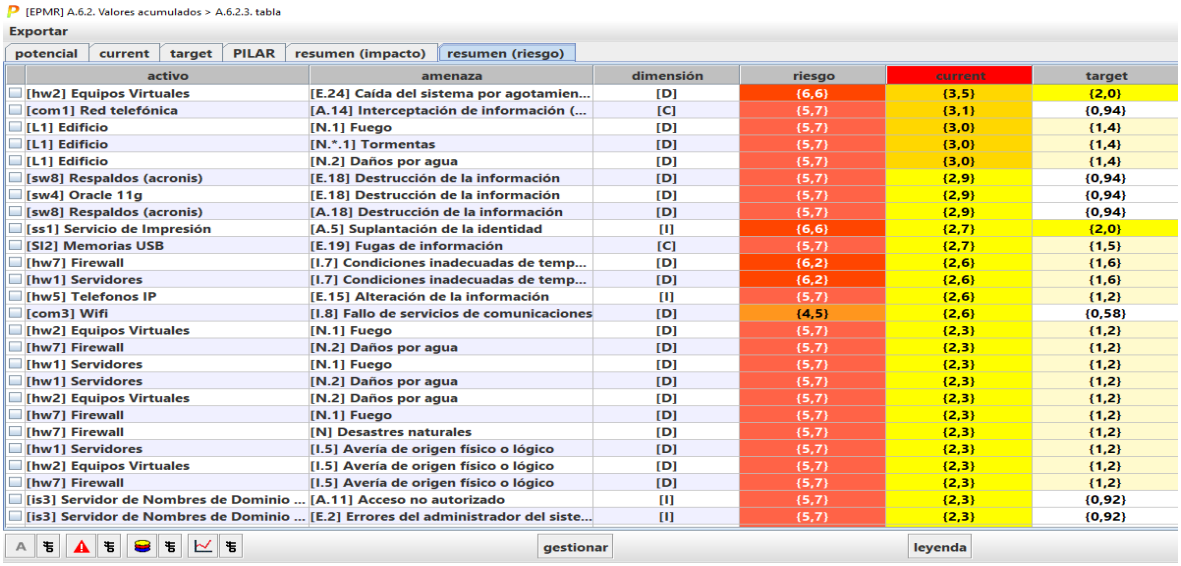
4.4. *Resumen de Resultados esperados*

El resumen de los resultados que se esperaban luego de aplicar las medidas de tratamiento de riesgo y el plan de seguridad se los puede visualizar en la Figura 27 donde se

compara el riesgo potencial, el riesgo actual y el riesgo objetivo y se visualiza la reducción del riesgo a medida que se implementan las salvaguardas.

Figura 27

Resumen Riesgo



[EPMR] A.6.2. Valores acumulados > A.6.2.3. tabla

Exportar

potencial | current | target | PILAR | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	riesgo	current	target
[hw2] Equipos Virtuales	[E.24] Caída del sistema por agotamien...	[D]	{6,6}	{3,5}	{2,0}
[com1] Red telefónica	[A.14] Interceptación de información (...	[C]	{5,7}	{3,1}	{0,94}
[L1] Edificio	[N.1] Fuego	[D]	{5,7}	{3,0}	{1,4}
[L1] Edificio	[N.*.1] Tormentas	[D]	{5,7}	{3,0}	{1,4}
[L1] Edificio	[N.2] Daños por agua	[D]	{5,7}	{3,0}	{1,4}
[sw8] Respaldos (acronis)	[E.18] Destrucción de la información	[D]	{5,7}	{2,9}	{0,94}
[sw4] Oracle 11g	[E.18] Destrucción de la información	[D]	{5,7}	{2,9}	{0,94}
[sw8] Respaldos (acronis)	[A.18] Destrucción de la información	[D]	{5,7}	{2,9}	{0,94}
[ss1] Servicio de Impresión	[A.5] Suplantación de la identidad	[I]	{6,6}	{2,7}	{2,0}
[SI2] Memorias USB	[E.19] Fugas de información	[C]	{5,7}	{2,7}	{1,5}
[hw7] Firewall	[I.7] Condiciones inadecuadas de temp...	[D]	{6,2}	{2,6}	{1,6}
[hw1] Servidores	[I.7] Condiciones inadecuadas de temp...	[D]	{6,2}	{2,6}	{1,6}
[hw5] Telefonos IP	[E.15] Alteración de la información	[I]	{5,7}	{2,6}	{1,2}
[com3] Wifi	[I.8] Fallo de servicios de comunicaciones	[D]	{4,5}	{2,6}	{0,58}
[hw2] Equipos Virtuales	[N.1] Fuego	[D]	{5,7}	{2,3}	{1,2}
[hw7] Firewall	[N.2] Daños por agua	[D]	{5,7}	{2,3}	{1,2}
[hw1] Servidores	[N.1] Fuego	[D]	{5,7}	{2,3}	{1,2}
[hw1] Servidores	[N.2] Daños por agua	[D]	{5,7}	{2,3}	{1,2}
[hw2] Equipos Virtuales	[N.2] Daños por agua	[D]	{5,7}	{2,3}	{1,2}
[hw7] Firewall	[N.1] Fuego	[D]	{5,7}	{2,3}	{1,2}
[hw7] Firewall	[N] Desastres naturales	[D]	{5,7}	{2,3}	{1,2}
[hw1] Servidores	[I.5] Avería de origen físico o lógico	[D]	{5,7}	{2,3}	{1,2}
[hw2] Equipos Virtuales	[I.5] Avería de origen físico o lógico	[D]	{5,7}	{2,3}	{1,2}
[hw7] Firewall	[I.5] Avería de origen físico o lógico	[D]	{5,7}	{2,3}	{1,2}
[is3] Servidor de Nombres de Dominio ...	[A.11] Acceso no autorizado	[I]	{5,7}	{2,3}	{0,92}
[is3] Servidor de Nombres de Dominio ...	[E.2] Errores del administrador del siste...	[I]	{5,7}	{2,3}	{0,92}

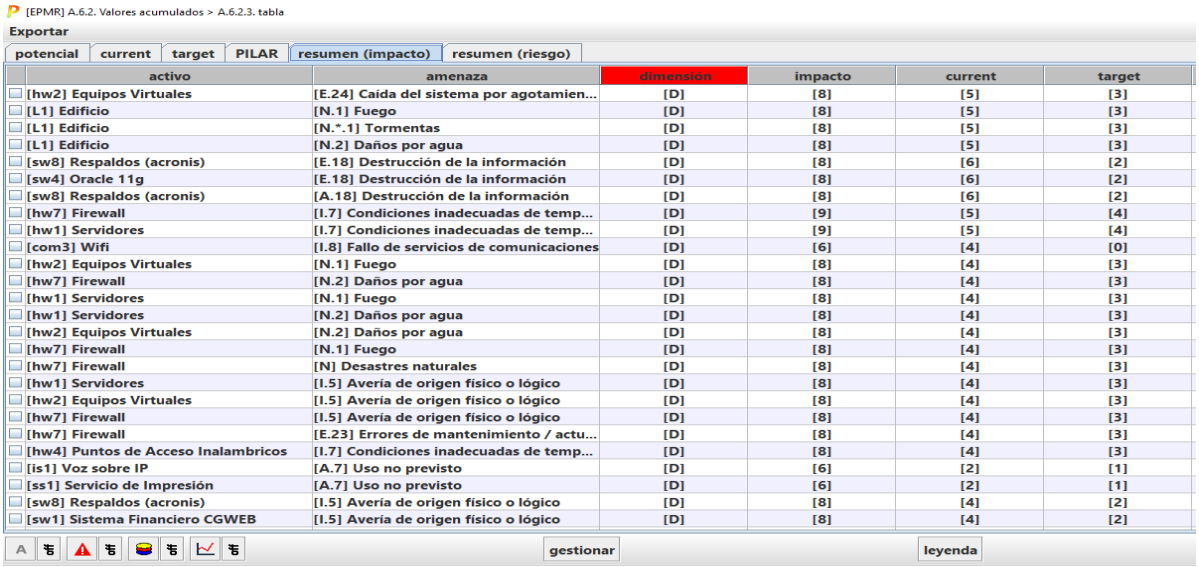
A | gestionar | leyenda

Nota. Evolución del estado de riesgo del proyecto. Elaborador por Autores en PILAR

Lo mismo se puede apreciar en la reducción del impacto en la Figura 28 al comparar el impacto potencial, el actual y el target.

Figura 28

Resumen Impacto



[EPMR] A.6.2. Valores acumulados > A.6.2.3. tabla

Exportar

potencial | current | target | PILAR | resumen (impacto) | resumen (riesgo)

activo	amenaza	dimensión	impacto	current	target
[hw2] Equipos Virtuales	[E.24] Caída del sistema por agotamien...	[D]	[8]	[5]	[3]
[L1] Edificio	[N.1] Fuego	[D]	[8]	[5]	[3]
[L1] Edificio	[N.*.1] Tormentas	[D]	[8]	[5]	[3]
[L1] Edificio	[N.2] Daños por agua	[D]	[8]	[5]	[3]
[sw8] Respaldos (acronis)	[E.18] Destrucción de la información	[D]	[8]	[6]	[2]
[sw4] Oracle 11g	[E.18] Destrucción de la información	[D]	[8]	[6]	[2]
[sw8] Respaldos (acronis)	[A.18] Destrucción de la información	[D]	[8]	[6]	[2]
[hw7] Firewall	[I.7] Condiciones inadecuadas de temp...	[D]	[9]	[5]	[4]
[hw1] Servidores	[I.7] Condiciones inadecuadas de temp...	[D]	[9]	[5]	[4]
[com3] Wifi	[I.8] Fallo de servicios de comunicaciones	[D]	[6]	[4]	[0]
[hw2] Equipos Virtuales	[N.1] Fuego	[D]	[8]	[4]	[3]
[hw7] Firewall	[N.2] Daños por agua	[D]	[8]	[4]	[3]
[hw1] Servidores	[N.1] Fuego	[D]	[8]	[4]	[3]
[hw1] Servidores	[N.2] Daños por agua	[D]	[8]	[4]	[3]
[hw2] Equipos Virtuales	[N.2] Daños por agua	[D]	[8]	[4]	[3]
[hw7] Firewall	[N.1] Fuego	[D]	[8]	[4]	[3]
[hw7] Firewall	[N] Desastres naturales	[D]	[8]	[4]	[3]
[hw1] Servidores	[I.5] Avería de origen físico o lógico	[D]	[8]	[4]	[3]
[hw2] Equipos Virtuales	[I.5] Avería de origen físico o lógico	[D]	[8]	[4]	[3]
[hw7] Firewall	[I.5] Avería de origen físico o lógico	[D]	[8]	[4]	[3]
[hw7] Firewall	[E.23] Errores de mantenimiento / actu...	[D]	[8]	[4]	[3]
[hw4] Puntos de Acceso Inalambricos	[I.7] Condiciones inadecuadas de temp...	[D]	[8]	[4]	[3]
[is1] Voz sobre IP	[A.7] Uso no previsto	[D]	[6]	[2]	[1]
[ss1] Servicio de Impresión	[A.7] Uso no previsto	[D]	[6]	[2]	[1]
[sw8] Respaldos (acronis)	[I.5] Avería de origen físico o lógico	[D]	[8]	[4]	[2]
[sw1] Sistema Financiero CGWEB	[I.5] Avería de origen físico o lógico	[D]	[8]	[4]	[2]

A | gestionar | leyenda

Nota. Evolución del valor del impacto en el proyecto. Elaborador por Autores en PILAR

CONCLUSIONES

- Con la utilización de la herramienta PILAR fue factible listar los activos que posee el departamento de tecnología de la EPMR, de igual manera se identificaron las amenazas y el impacto que tendrían estas si es que llegaran a materializarse, todo esto fundamentados y siguiendo los lineamientos de la metodología MAGERIT.
- Mediante el reconocimiento e implementación de salvaguardas se logró verificar la reducción de los niveles de riesgo que tiene cada activo, de igual manera la implementación de controles necesarios que permitan mitigar o reducir el riesgo por ejemplo de errores no intencionados de configuración de administradores o incluso evitar fugas de información con mecanismos que disminuyan el riesgo a un nivel manejable.
- Se ha elaborado un plan de seguridad que contiene, un plan de ejecución y una política de seguridad, en el que intervienen personas de distintas áreas involucradas directamente con el propósito de implementar medidas preventivas y de ser el caso correctivas para reducir el riesgo existente.
- El proceso de gestión de riesgos debe considerarse como un aspecto fundamental en una empresa, esto debido a que, si no se conoce el riesgo al que puedan estar expuestos sus activos informáticos, muy difícil ayudará a evitar la posibilidad de que ocurra un incidente, por ello la importancia de conocer y establecer procesos que permitan mitigar o eliminar su ocurrencia.
- Luego de realizar el tratamiento de riesgos en los activos más críticos que en total fueron 20, se obtuvo como resultado la disminución significativa del riesgo en estos, únicamente en el tratamiento de 2 activos se redujo a nivel de criticidad medio que indica que se debe seguir trabajando para mitigar esos riesgos hasta llegar a un nivel

bajo o depreciable, de un total de 20 activos 18 fueron tratados con éxito representando el 90% de todos los activos.

- El desarrollo del presente proyecto sirve de manera objetiva para el encaminamiento de la seguridad y buenas prácticas acerca de la utilización de los recursos informáticos, mediante normativas y políticas que han sido orientadas a los funcionarios de la institución.

RECOMENDACIONES

- Se recomienda ejecutar un constante análisis de riesgos y amenazas que puedan ocurrir a futuro debido al gran cambio tecnológico que existe en la actualidad.
- Se sugiere realizar capacitaciones periódicas al personal con el fin de que conozcan las normas de seguridad y políticas establecidas en el presente documento.
- Se recomienda actualizar el plan de seguridad de manera periódica con el fin de mejorar o implementar nuevas soluciones óptimas que permitan optimizar la seguridad de los activos.
- Se recomienda que aquellos activos cuyo tratamiento de riesgo pueda ser transferido, se los considere dentro de un plan de protección con entidades certificadas como aseguradoras.

REFERENCIAS

Libros

Consejo Superior de Administración Electrónica. (2012a). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Consejo Superior de Administración Electrónica. (2012b). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas.*

Consejo Superior de Administración Electrónica. (2012c). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos*.

Daltabuit, E., Hernadez, L., Mallen, Gu., & Vazquez, J. de J. (2007). *Seguridad de la información*. Limusa. http://libgen.rs/book/index.php?md5=ED3DA81FEB6AD9CD55E1AAFDA6F11C89

Fabián, J., & Buendía, R. (2013). *Seguridad informática*. McGraw-Hill. www.mhe.es/cf/informaticawww.FreeLibros.me

Gutiérrez, C. (2020). *MAGERIT: metodología práctica para gestionar riesgos | WeLiveSecurity*. https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Ignacio, J., Fernández, V., Luis, J., & Cuadrado, L. (2015). *Plan de Contingencia de Tecnologías de la Información para entornos distriuidos*. https://e-archivo.uc3m.es/handle/10016/22424

López, A. (2010). *Seguridad informática*. Editex.

Nadia Belu. (2018). *ISO 31000:2018 - Risk management — Guidelines - ISO*.

Nicolás, F., Solarte, J. S., Rodrigo, E., Rosero, E., Del Carmen, M., & Ruano, B. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. In *Revista Tecnológica ESPOL-RTE* (Vol. 28, Issue 5). http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Organización Internacional de Normalización. (2005). *GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISO 27001)*. https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf

Artículos Científicos

- Sena, L., & Tenzer, S. M. (2004). Introducción a Riesgo informático. *Facultad de Ciencias Económicas y de Administración. Universidad de La República de Montevideo, Uruguay*, 16–17.
- Solarte, F. N. S., Rosero, E. R. E., & del Carmen Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL*, *28*(5).

Páginas WEB

- Gutiérrez, C. (2020). *MAGERIT: metodología práctica para gestionar riesgos | WeLiveSecurity*. https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/
- *RUMIÑAHUI – ASEO, EPM*. (n.d.). Retrieved January 24, 2021, from http://www.ruminahui-aseo.gob.ec/

Tesis

- Ignacio, J., Fernández, V., Luis, J., & Cuadrado, L. (2015). *Plan de Contingencia de Tecnologías de la Información para entornos distriuidos*. https://e-archivo.uc3m.es/handle/10016/22424

Normas

- Organización Internacional de Normalización. (2005). *GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ISO 27001)*. https://www.isotools.org/pdfs-pro/iso-27001-sistema-gestion-seguridad-informacion.pdf
- ISO. (2018). *ISO 31000:2018 - Risk management — Guidelines - ISO*.

ANEXOS

ANEXO A. DECLARACIÓN PERSONAL DE CONFIDENCIALIDAD Y PRIVACIDAD DE CONTRASEÑAS

En la parroquia de Sangolquí a los (# de día) días del mes de (mes) del año (año), comparecen los implicados para firmar el presente acuerdo de confidencialidad y privacidad para el manejo de contraseñas que permitan los accesos a los distintos servicios y sistemas brindados por el departamento de tecnología para realizar las labores que han sido asignadas por lo jefes de cada área considerando los siguientes aspectos:

- El funcionario se compromete a la creación de contraseñas robustas siguiendo las normativas indicadas por el personal de tecnología.
- El funcionario se compromete a comunicar al departamento de tecnología en caso de sospechar el robo o perdida de contraseñas.
- El funcionario se compromete a no divulgar por ningún motivo sus contraseñas personales a los demás usuarios.

Para constancia las partes firman 2 ejemplares con la misma validez.

_____	_____
Nombre del Funcionario	Jefe de Tecnología

ANEXO B POLÍTICA DE SEGURIDAD

1.- **Introducción**

El departamento de tecnología e información y comunicaciones pertenece a la Gerencia de Planificación y Gestión empresarial, cuenta con un Jefe de Tecnología y un Técnico en Informática, que son los encargados de brindar los servicios tecnológicos a los funcionarios de la Empresa Pública Municipal de Residuos Sólidos Rumiñahui Aseo (EPMR) de aquí en adelante.

La presente política de seguridad cubre muchos factores referentes a la seguridad de la información y de recursos informáticos.

2.- **Objetivo**

Establecer una normativa para el correcto uso de los servicios y recursos informáticos de la EPMR por parte de los funcionarios en sus actividades laborales.

3.- **Alcance**

Esta política, está orientada a los funcionarios de la EPMR que hagan uso de los servicios que ofrece el departamento de tecnología.

El departamento de tecnología será el encargado de administrar, actualizar, modificar la presente política dependiendo de la necesidad propia de la institución.

La presente política puede ser aplicada en los activos informáticos de la empresa, de igual manera en funcionarios o personas ajenas a la institución quienes requieran de los servicios o recursos informáticos de la EPMR.

4.- Utilización del presente documento

El presente documento sirve como guía para el buen uso de recursos informáticos basados en políticas de seguridad que garanticen la continuidad de los servicios y operación de los equipos informáticos.

5.- **Definición de Políticas**

GENERALES

El departamento de tecnología es responsable de:

1. Velar por los servicios y recursos informáticos de la institución.
2. El área de activos fijos será el responsable de llevar un control de los equipos que sean entregados a los funcionarios, así como de coordinar con el departamento de tecnología sobre los activos informáticos existentes.
3. Por ningún motivo los funcionarios de la empresa malgastarán los recursos informáticos para realizar actividades personales o que no pertenezcan a las actividades propias de la institución.
4. El departamento de tecnología mediante su mesa de ayuda será el único encargado de gestionar el soporte técnico en los equipos informáticos de la empresa.

RESPALDO DE LA INFORMACIÓN

1. Es responsabilidad del personal de tecnología verificar la información crítica que tienen a su cargo para generar crear copias de seguridad de respaldos de la información.
2. El personal de tecnología es el encargado de velar por el funcionamiento y buena ejecución del software de respaldo y restauración, que permite realizar las copias de seguridad de los dispositivos informáticos.
3. La información que se respalde debe ser la obtenida de los siguientes equipos:

- Equipos Servidores virtuales y físicos.
- Estaciones de trabajo personales.
- Equipos de comunicación.

4. Los tipos de respaldo incremental (diario) o completo (semanal) que se deben realizar en los equipos informáticos son los siguientes:
   - Equipos servidores virtuales y físicos (incremental y completo).
   - Estaciones de trabajo (incremental y completo).
   - Equipos de comunicación (completo, conforme se realice algún cambio en la configuración).
5. El personal de tecnología será el encargado de planificar el horario de ejecución de respaldos con el objetivo de que este no interfiera en las actividades diarias de los funcionarios.
6. Para el respaldo considerar por lo menos 3 lugares en donde se pueda almacenar la información, la primera en el servidor destinado al respaldo de la información, la segunda almacenamiento en la nube y la tercera enviar copias físicas de los respaldos a otra entidad con la que se tenga algún acuerdo.
7. El personal del departamento de tecnología será el encargado de comprobar el espacio de almacenamiento en el disco del servidor y en caso de necesitar espacio se deberá respaldar esa información en medios físicos para enviar a otra entidad.
8. El personal del departamento de tecnología será el encargado de gestionar nuevos agentes de copia de seguridad en el caso de que existieran más servidores o estaciones de trabajo.
9. En el caso de pérdida de la información el personal de tecnología será el encargado de autorizar las solicitudes de respaldo y restauración de las mismas.

EQUIPAMIENTO INFORMÁTICO

Instalación de Equipos informáticos

1. Todo equipo adquirido o inventariado en la EPMR debe tener un código de bien único que juntamente con el área de activos fijos deben llevarse el control.
2. En área de tecnología debe generar un conjunto de normas y procedimientos que permita la instalación de equipamiento informáticos como servidores, equipos de cómputo y este debe ser cumplido estrictamente.
3. Los equipos considerados para la prestación de servicios críticos deben encontrarse en un área segura, a la que sea difícil el acceso de personas no autorizadas, con las características indispensables de seguridad física, alimentación eléctrica redundante, buenas condiciones ambientales y el control del acceso por parte del personal de tecnología.
4. Los equipos de cómputo no deben ser movidos o reubicados por el resto del personal administrativo, este tiene que ser comunicado a los funcionarios del departamento de tecnología para verificar si es viable la reubicación

Mantenimiento de los equipos informáticos

1. El técnico en informática es el responsable directo de velar por el estado y funcionamiento de los equipos, para ello debe realizar el mantenimiento preventivo y correctivo de los equipos informáticos, de igual manera asegurarse de la instalación y seguridad física.
2. El personal técnico no efectuará trabajos en equipos de cómputo que no sean de la empresa, no tiene autorización de realizar trabajos de mantenimientos en los equipos mencionados.

Reubicación de equipos informáticos

1. El área técnica del departamento de tecnología es la responsable de la verificación de la viabilidad para la reubicación de un equipo informático, cumpliendo con normas que garanticen el correcto funcionamiento de los equipos.
2. En caso de existir reasignación de equipos, por distintos factores como compra de nuevos equipos o designación a nuevas personas de equipos ya existentes, es necesario comunicar con el departamento de tecnología para socializar con el responsable de activos fijos el cambio de custodio y realizar el registro del cambio.
3. Todo cambio de ubicación de equipos informáticos deberá constar con la aprobación de los Gerentes de cada área y del Jefe de Tecnología.

CONTROL DE ACCESOS

Acceso a áreas restringidas

1. Llevar un registro obligatorio de acceso del personal interno y externo a las áreas consideradas como críticas en la empresa tanto al momento de ingreso como al de salida.
2. El departamento de tecnología es el responsable de asegurar el perímetro físico y de ingreso a las instalaciones, considerando la infraestructura de seguridad pertinente sin escatimar costos.
3. Para acceder a las instalaciones donde se encuentren equipos tecnológicos, el acceso a personas ajenas deberá obligatoriamente verse acompañado de un funcionario del departamento de tecnología.

Acceso al equipamiento informático

1. Cada equipo informático de la empresa es asignado a un funcionario, este es el responsable de velar por el estado del equipo y hacer buen uso del mismo.
2. Los equipos de cómputo de la empresa serán utilizados únicamente para realizar labores planteadas por la organización.

3. En los equipos de comunicación como firewall, switch, Access point, servidores, etc., el acceso lógico es únicamente por parte del personal de tecnología que son los encargados de administrar los equipos.
4. En caso de daño o avería del equipo de cómputo es obligatoriamente necesario comunicar al departamento de tecnología sobre el suceso para realizar las correcciones pertinentes.
5. Queda prohibida la instalación de software ajeno a la institución sin previa autorización por el departamento de tecnología.

Acceso a la red

1. El departamento de tecnología es el responsable de brindar el acceso a los recursos de la red.
2. El departamento de tecnología es el responsable de difundir el buen uso de la red y de velar por su cumplimiento.
3. En caso de requerir conectar a la red interna un equipo de cómputo que no pertenezca a la empresa, deberá solicitar el permiso necesario al departamento de tecnología con el fin de verificar que el equipo no presenta riesgo alguno para la seguridad de la red.
4. En caso de requerir permiso total para la navegación por internet, debe solicitar la autorización al departamento de tecnología con la debida justificación que requiere para realizar el trabajo pertinente autorizado por el jefe de cada área.
5. Los equipos de cómputo conectados a la red de la empresa deberán contar con un fondo de pantalla definido por el departamento de tecnología en donde haga referencia a información de la empresa aprobada por la máxima autoridad.
6. Por ningún motivo está permitido la descarga de videos o música desde internet sin previa justificación y autorización.

Acceso a Sistemas Informáticos

1. El acceso a los sistemas informáticas por parte del personal administrativo será autorizado por el jefe de área y deberá definirse roles y permisos para los sistemas por parte del departamento de tecnología.
2. El acceso a servidores de bases de datos está prohibido para personal no autorizado por ser un servicio dedicado.
3. Por ningún motivo se podrá hacer uso de un sistema informático de la empresa para recabar información y divulgarla sin autorización previa.
4. Es obligación del funcionario cerrar sesión de cualquier sistema informático para evitar accesos no autorizados a los mismos.

GESTIÓN DE CONTRASEÑAS

- Los funcionarios de la empresa tienen responsabilidad directa para cuidar responsablemente de sus contraseñas que tiene a su cargo para el acceso a los recursos o sistemas informáticos proporcionados.
- Se considera que las contraseñas son de uso personal y por tanto son intransferibles.
- El cambio de contraseñas se lo realizará con un periodo de al menos una vez cada 3 meses en los sistemas tanto en cuentas de administrador y cuentas de usuario.
- Las contraseñas utilizadas deberán tener un mínimo de 8 caracteres entre mayúsculas y minúsculas combinadas con números y obligatoriamente un carácter especial como (.,-+%$#), no hacer referencia a nombres personales o de usuario. Ej.: Passw0rd$
- Si hubiera sospecha de utilización de alguna contraseña personal por parte de otro funcionario ajeno a la misma, se deberá comunicar al departamento de tecnología para cambiarle de forma urgente.

- Por ningún motivo una contraseña creada debe ser revelada por algún medio electrónico como chat o correo electrónico ni por medio telefónico.

GESTIÓN DE LA INFORMACIÓN

1. Todo funcionario que tenga a su cargo un equipo informático debe estar consciente que la creación o modificación de la información en sistemas o aplicaciones de la empresa, así mismo como en soportes de información electrónica como discos duros externos o memorias USB, en el desarrollo de las actividades de la empresa, son propiedad netamente de la organización.
2. Toda creación de matrices en hojas de cálculos, desarrollo de software o documentación electrónica realizada por los funcionarios se considera de propiedad absoluta de la institución.
3. El departamento de tecnología es el encargado de resguardar los respaldos de la información de cada funcionario mediante copias de seguridad periódicas.

USO DE SOFTWARE

10. El departamento de tecnología deberá ser el único encargado de la instalación, administración y ejecución o solicitud de soporte en caso de requerirlo del software instalado.
11. Todo software utilizado por los funcionarios debe ser exclusivamente para actividades relacionadas con la institución.
12. El departamento de tecnología es el encargado de llevar un control de renovación de licencias que se encuentran en operación con el fin de continuar con los servicios.
13. Por ningún motivo se podrá instalar software descargado de internet por parte de los funcionarios sin previa autorización por el departamento de tecnología.
14. Las actualizaciones de software serán administradas por el departamento de tecnología.

6.- Implementación de la Políticas

En cuanto a la vigencia de las políticas descritas anteriormente, dependerá de la aprobación de la máxima autoridad de la empresa y serán revisadas, actualizadas o corregidas por el personal de tecnología de la institución.

7.- Sanciones por incumplimiento

El desconocer las políticas detalladas en este documento no exime de responsabilidad a los funcionarios de la institución que tendrán que aceptar las siguientes sanciones:

1. Cualquier política violada deberá ser sancionada conforme al reglamento interno de la institución.
2. En caso de incumplir con las políticas mencionadas se notificará del hecho y de ser el caso se procederá a la suspensión temporal de los servicios o equipos informáticos con el debido consentimiento de la máxima autoridad.
3. En caso de reincidencia, se procede a la comunicación del hecho al departamento Administrativo y de Talento Humano para que actúen de acuerdo a las normas establecidas.

ANEXO C IDENTIFICACIÓN DE LOS ACTIVOS

[B]ACTIVOS ESENCIALES

- [E1] Información confidencial.

[IS] SERVICIOS INTERNOS

Como servicios se puede indicar que en la EPMR para los usuarios internos se tienen los siguientes:

- [is1] Voz sobre IP
- [is2] Internet
- [is3] soporte al usuario
- [is4] servidor de nombres de dominio

[SS]SERVICIOS SUBCONTRATADOS

- [ss1] impresión
- [ss2] alojamiento de servidor Web
- [ss3] Correo Electrónico
- [ss4] proveedor de servicio de internet
- [ss5] respaldo de datos
- [ss6] alojamiento de aplicaciones

[SW]APLICACIONES (Software)

Entre las aplicaciones que cuenta la institución se puede mencionar las siguientes:

- [sw1] Sistema Financiero CGWEB
- [sw2] Ofimática
- [sw3] servidor de directorio

- [sw4] sistema de gestión de base de datos (Oracle 11g)
- [sw5] sistema operativo (windows, linux)
- [sw6] hipervisor (gestor de la máquina virtual)
- [sw7]Sistema de Gestión Documental RUMIDOCS
- [sw8] Respaldos (Acronis)
- [sw9] Antivirus (ESET)
- [sw10] Monitoreo de Red (PRTG)
- [sw11] Sophos SSL VPN Client

[HW] EQUIPAMIENTO INFORMÁTICOS (HARDWARE)

Se consideran los siguientes equipos informáticos que posee la empresa:

- [hw1]Servidores
- [hw2] Equipos Virtuales
- [hw3]Conmutador
- [hw4] punto de acceso Wireless
- [hw5] Teléfonos ip
- [hw6] informática personal (Computadores Todo en Uno, computador de escritorio, laptops)

[COM] REDES DE COMUNICACIONES

Para la comunicación y transporte de información se tiene los siguientes medios:

- [com1] Red telefónica
- [com2] red de datos
- [com3] wifi
- [com4] red local

- [com5] red virtual
- [com6] VPN

[SI] SOPORTES DE INFORMACIÓN

En la EPMR se utiliza los siguientes dispositivos como soporte de información:

- [SI3]discos
- [SI1] memorias USB
- [SI2] material impreso

[AUX] EQUIPAMIENTO AUXILIAR

Como equipo auxiliar la EPMR cuenta con el siguiente equipamiento:

- [aux1] Equipos de climatización
- [aux2] Fuentes de alimentación
- [aux3] cableado de datos (fibra y de alimentación)
- [aux4] sistema de alimentación interrumpida
- [aux5] sistema de video vigilancia

[L] INSTALACIONES

La infraestructura tecnológica de la Empresa Pública Municipal de Residuos Sólidos Rumiñahui Aseo EPM, se encuentra ubicada dentro de las dependencias de la empresa en la Av. Gral. Enríquez s/n, vía a Cotogchoa, cuenta con un centro de datos principal, otro ubicado en la instalaciones de la Radio Ecos de Rumiñahui y racks ubicados en las distintas gerencias con los equipos de comunicación.

- [i1] edificio

[P] PERSONAL

En el siguiente apartado se puede identificar a las personas relacionas con los sistemas de información que pertenecen al Departamento de Tecnología de la Información y Comunicación.

Dentro del personal se puede indicar los siguientes miembros del área:

- [p2]administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.
- [p1]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática

ANEXO D AMENAZAS SOBRE CADA ACTIVO

ACTIVOS	AMENAZAS
Información Confidencial	[E.1] Errores de los usuarios
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.15] Alteración de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de información
	[A.5] Suplantación de la identidad
	[A.6] Abuso de privilegios de acceso
	[A.11] Acceso no autorizado
	[A.15] Modificación de la información
	[A.18] Destrucción de la información
	[A.19] Revelación de información
Voz Sobre IP	[E.1] Errores de los usuarios
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.5] Suplantación de la identidad
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.13] Repudio (negación de actuaciones)
	[A.24] Denegación de servicio
Internet	[A.7] Uso no previsto
Soporte al Usuario	[E.1] Errores de los usuarios
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.15] Alteración de la información
	[E.18] Destrucción de la información
	[E.19] Fugas de información
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.13] Repudio (negación de actuaciones)
	[A.24] Denegación de servicio
Servidor de Nombres de Dominio DNS	[E.1] Errores de los usuarios
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.13] Repudio (negación de actuaciones)
	[A.24] Denegación de servicio
[ss1] Servicio de Impresión	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.9] Errores de [re-]encaminamiento

	[E.10] Errores de secuencia
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.9] [Re-]encaminamiento de mensajes
	[A.11] Acceso no autorizado
	[A.13] Repudio
[ss2] Alojamiento de servidor Web	[E.2] Errores del administrador
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de secuencia
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
	[A.15] Modificación deliberada de la información
	[A.18] Destrucción de información
	[A.19] Divulgación de información
[ss3] Correo Electrónico	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.9] Errores de [re-]encaminamiento
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
	[A.13] Repudio
	[A.15] Modificación deliberada de la información
	[A.18] Destrucción de información
	[A.19] Divulgación de información
[ss4] Proveedor de servicio de internet	[E.2] Errores del administrador
	[A.7] Uso no previsto
[ss5] Respaldo de datos	[E.2] Errores del administrador
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
	[A.15] Modificación deliberada de la información
	[A.18] Destrucción de información
	[A.19] Divulgación de información
[ss6] Alojamiento de aplicaciones (Hosting)	[I.5] Avería de origen físico o lógico
	[E.1] Errores de los usuarios

	[E.2] Errores del administrador
[sw1] Sistema Financiero CGWEB	[I.5] Avería de origen físico o lógico
	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
[sw2] Microsoft Office	[I.5] Avería de origen físico o lógico
	[E.1] Errores de los usuarios
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.8] Difusión de software dañino
[sw3] Active Directory	[E.2] Errores del administrador
	[E.8] Difusión de software dañino
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de secuencia
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.5] Suplantación de la identidad del usuario
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.8] Difusión de software dañino
	[A.9] [Re-]encaminamiento de mensajes
	[A.11] Acceso no autorizado
	[A.15] Modificación deliberada de la información
	[A.18] Destrucción de información
	[A.19] Divulgación de información
	[A.22] Manipulación de programas
[sw4] Oracle 11g	[E.2] Errores del administrador
	[E.8] Difusión de software dañino
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.7] Uso no previsto
	[A.8] Difusión de software dañino
	[A.19] Divulgación de información

	[A.22] Manipulación de programas
[sw5] Sistemas Operativos (Windows, Linux)	[I.5] Avería de origen físico o lógico
	[E.1] Errores de los usuarios
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.7] Uso no previsto
[sw6] Hipervisor (gestor de la máquina virtual)	[I.5] Avería de origen físico o lógico
	[E.2] Errores del administrador
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
[sw7] Sistema de Gestión Documental RUMIDOCS	[I.5] Avería de origen físico o lógico
	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.5] Suplantación de la identidad del usuario
[sw8] Respaldos (acronis)	[I.5] Avería de origen físico o lógico
	[E.2] Errores del administrador
	[E.15] Alteración accidental de la información
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.18] Destrucción de información
	[A.19] Divulgación de información
	[A.22] Manipulación de programas
[sw9] Antivirus ESET	[E.2] Errores del administrador
	[E.8] Difusión de software dañino
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
[sw10] Monitoreo de Red PRTG	[I.5] Avería de origen físico o lógico
	[E.19] Fugas de información
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.9] [Re-]encaminamiento de mensajes
	[I.5] Avería de origen físico o lógico

[sw11] Sophos SSL VPN Client	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.20] Vulnerabilidades de los programas (software)
	[E.21] Errores de mantenimiento / actualización de programas (software)
	[A.5] Suplantación de la identidad del usuario
	[A.7] Uso no previsto
	[A.11] Acceso no autorizado
[hw1]Servidores	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
[hw2] Equipos Virtuales	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.23] Errores de mantenimiento / actualización de equipos
	[E.24] Caída del sistema por agotamiento de recursos
	[A.11] Acceso no autorizado
[hw3]Conmutador	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.11] Acceso no autorizado
[hw4] punto de acceso inalámbricos	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[A.11] Acceso no autorizado
[hw5] teléfonos ip	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales

	[I.5] Avería de origen físico o lógico
	[I.8] Fallo de servicios de comunicaciones
	[E.9] Errores de [re-]encaminamiento
	[E.15] Alteración de la información
	[E.19] Fugas de información
	[A.7] Uso no previsto
	[A.9] [Re-]encaminamiento de mensajes
	[A.14] Interceptación de información (escucha)
[hw6] informática personal (Computadores Todo en Uno, computador de escritorio, laptops)	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.*] Desastres industriales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[E.24] Caída del sistema por agotamiento de recursos
	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
hw7 Firewall	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.7] Condiciones inadecuadas de temperatura o humedad
	[E.2] Errores del administrador del sistema / de la seguridad
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)
	[A.11] Acceso no autorizado
	[A.23] Manipulación del hardware
[com1] red telefónica	[N.1] Fuego
	[N.2] Daños por agua
	[N.*] Desastres naturales
	[I.5] Avería de origen físico o lógico
	[I.8] Fallo de servicios de comunicaciones
	[A.14] Interceptación de información (escucha)
[com2] red de datos	[I.8] Fallo de servicios de comunicaciones
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de secuencia
	[A.9] [Re-]encaminamiento de mensajes
	[A.11] Acceso no autorizado
[com3] wifi	[I.8] Fallo de servicios de comunicaciones
	[E.9] Errores de [re-]encaminamiento
[com4] red local	[I.8] Fallo de servicios de comunicaciones
	[E.9] Errores de [re-]encaminamiento

	[E.10] Errores de secuencia
	[A.5] Suplantación de la identidad del usuario
	[A.9] [Re-]encaminamiento de mensajes
	[A.11] Acceso no autorizado
[com5] red virtual	[I.8] Fallo de servicios de comunicaciones
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de secuencia
	[A.9] [Re-]encaminamiento de mensajes
	[A.11] Acceso no autorizado
[com6] VPN	[I.8] Fallo de servicios de comunicaciones
	[E.9] Errores de [re-]encaminamiento
	[E.10] Errores de secuencia
	[A.5] Suplantación de la identidad del usuario
	[A.11] Acceso no autorizado
[SI1]discos	[E.15] Alteración de la información
	[E.19] Fugas de información
	[A.15] Modificación de la información
	[A.19] Revelación de información
[SI2] memorias USB	[E.15] Alteración de la información
	[E.19] Fugas de información
	[A.15] Modificación de la información
	[A.19] Revelación de información
[SI3] material impreso	[E.15] Alteración de la información
	[E.19] Fugas de información
	[A.15] Modificación de la información
	[A.19] Revelación de información
[aux1] Equipos de climatización	[I.3] Contaminación medioambiental
[aux2] Fuentes de alimentación	[I.3] Contaminación medioambiental
[aux3] cableado de datos (fibra y de alimentación)	[I.3] Contaminación medioambiental
	[I.7] Condiciones inadecuadas de temperatura o humedad
[aux4] sistema de alimentación interrumpida	[I.3] Contaminación medioambiental
[aux5] Sistema de video vigilancia	[I.3] Contaminación medioambiental
	[I.7] Condiciones inadecuadas de temperatura o humedad
[i1] edificio	[N.1] Fuego
	[N.2] Daños por agua
	[N.*.1] Tormentas
	[N.*.4] Terremotos
	[I.*] Desastres Industriales
	[E.4] Errores de configuración

[p2]administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.	[E.19] Fuga de información
	[E.28] Indisponibilidad del personal
	[A.29] Extorsión
[p1]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática	[E.4] Errores de configuración
	[E.19] Fuga de información
	[E.28] Indisponibilidad del personal
	[A.29] Extorsión

ANEXO E VALORACIÓN DE LAS AMENAZAS

ACTIVOS	AMENAZAS	P	[D]	[I]	[C]	[A]	[T]
Información Confidencial	[E.1] Errores de los usuarios	B	MA	MA	A	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	B	MA	MA	A	-	-
	[E.15] Alteración de la información	B	MA	MA	A	-	-
	[E.18] Destrucción de la información	B	MA	MA	A	-	-
	[E.19] Fugas de información	B	MA	MA	A	-	-
	[A.5] Suplantación de la identidad	B	MA	MA	A	-	-
	[A.6] Abuso de privilegios de acceso	B	MA	MA	A	-	-
	[A.11] Acceso no autorizado	B	MA	MA	A	-	-
	[A.15] Modificación deliberada de la información	B	MA	MA	A	-	-
	[A.18] Destrucción de información	B	MA	MA	A	-	-
	[A.19] Divulgación de información	B	MA	MA	A	-	-
Voz Sobre IP	[E.1] Errores de los usuarios	PP	M	B	B	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	-	-
	[E.19] Fugas de información	P	-	-	M	-	-
	[E.24] Caída del sistema por agotamiento de recursos	P	M	-	-	-	-
	[A.5] Suplantación de la identidad	PP	.	M	M	M	-
	[A.7] Uso no previsto	MA	M	M	M	-	-
	[A.11] Acceso no autorizado	P	-	B	B	-	-
	[A.13] Repudio (negación de actuaciones)	P	-	B	-	-	-
	[A.24] Denegación de servicio	PP	M	-	-	-	-

Internet	[A.7] Uso no previsto	PP	B	B	B	-	-
Soporte al Usuario	[E.1] Errores de los usuarios	PP	B	B	B	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	PP	M	B	B	-	-
	[E.15] Alteración de la información	PP	-	B	-	-	-
	[E.18] Destrucción de la información	PP	M	-	-	-	-
	[E.19] Fugas de información	PP	-	-	B	-	-
	[A.7] Uso no previsto	P	B	M	M	-	-
	[A.11] Acceso no autorizado	P	-	B	B	-	-
	[A.13] Repudio (negación de actuaciones)	PP	-	B	-	-	-
	[A.24] Denegación de servicio	PP	B	-	-	-	-
Servidor de Nombres de Dominio DNS	[E.1] Errores de los usuarios	PP	B	B	B	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	P	A	A	A	-	-
	[E.24] Caída del sistema por agotamiento de recursos	P	M	-	-	-	-
	[A.11] Acceso no autorizado	P	-	A	A	-	-
	[A.13] Repudio (negación de actuaciones)	P	-	M	-	-	-
	[A.24] Denegación de servicio	P	M	-	-	-	-
[ss1] Servicio de Impresión	[E.1] Errores de los usuarios	PP	B	B	B	-	-
	[E.2] Errores del administrador	PP	B	B	B	-	-
	[E.9] Errores de [re-]encaminamiento	PP	-	-	B	-	-
	[E.10] Errores de secuencia	PP	-	B	-	-	-
	[E.18] Destrucción de información	PP	B	-	-	-	-
	[E.19] Fugas de información	PP	-	-	B	-	-

	[E.24] Caída del sistema por agotamiento de recursos	P	M	-	-	-	-
	[A.5] Suplantación de la identidad del usuario	MA	M	A	M	-	-
	[A.6] Abuso de privilegios de acceso	P	B	M	B	-	-
	[A.7] Uso no previsto	MA	M	M	M	-	-
	[A.9] [Re-]encaminamiento de mensajes	PP	-	-	B	-	-
	[A.11] Acceso no autorizado	P	-	B	M	-	-
	[A.13] Repudio	PP	-	B	-	-	-
[ss2] Alojamiento de servidor Web	[E.2] Errores del administrador	P	A	A	A	-	-
	[E.9] Errores de [re-]encaminamiento	PP	-	-	B	-	-
	[E.10] Errores de secuencia	PP	-	B	-	-	-
	[E.15] Alteración accidental de la información	P	-	M	-	-	-
	[E.18] Destrucción de información	P	A	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	P	M	-	-	-	-
	[A.11] Acceso no autorizado	P	-	M	M	-	-
	[A.15] Modificación deliberada de la información	P	-	M	-	-	-
	[A.18] Destrucción de información	P	M	-	-	-	-
	[A.19] Divulgación de información	P	-	-	M	-	-
[ss3] Correo Electrónico	[E.1] Errores de los usuarios	PP	M	B	B	-	-
	[E.2] Errores del administrador	PP	B	B	B	-	-
	[E.9] Errores de [re-]encaminamiento	PP	-	-	B	-	-
	[E.18] Destrucción de información	P	M	-	-	-	-
	[E.19] Fugas de información	P	-	-	M	-	-

	[E.24] Caída del sistema por agotamiento de recursos	P	M	-	-	-	-
	[A.13] Repudio	PP	-	B	-	-	-
	[A.15] Modificación deliberada de la información	PP	-	B	-	-	-
	[A.18] Destrucción de información	P	M	-	-	-	-
	[A.19] Divulgación de información	P	-	-	M	-	-
[ss4] Proveedor de servicio de internet	[E.2] Errores del administrador	PP	M	B	B	-	-
	[A.7] Uso no previsto	PP	B	B	B	-	-
[ss5] Respaldo de datos	[E.2] Errores del administrador	P	M	B	B	-	-
	[E.15] Alteración accidental de la información	PP	-	B	-	-	-
	[E.18] Destrucción de información	PP	B	-	-	-	-
	[E.19] Fugas de información	PP	-	-	B	-	-
	[A.7] Uso no previsto	PP	B	B	B	-	-
	[A.11] Acceso no autorizado	PP	-	B	B	-	-
	[A.15] Modificación deliberada de la información	PP	-	B	-	-	-
	[A.18] Destrucción de información	PP	M	-	-	-	-
	[A.19] Divulgación de información	PP	-	-	M	-	-
[ss6] Alojamiento de aplicaciones (Hosting)	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[E.1] Errores de los usuarios	PP	M	B	B	-	-
	[E.2] Errores del administrador	PP	M	B	B	-	-
[sw1] Sistema Financiero CGWEB	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[E.1] Errores de los usuarios	P	M	M	M	-	-
	[E.2] Errores del administrador	P	M	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software)	PP	M	M	B	-	-

	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	-	-	-
[sw2] Microsoft Office	[I.5] Avería de origen físico o lógico	PP	M	-	-	-	-
	[E.1] Errores de los usuarios	P	M	M	M	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	B	M	B	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	B	M	-	-	-
	[A.8] Difusión de software dañino	PP	B	B	B	-	-
[sw3] Active Directory	[E.2] Errores del administrador	P	M	M	M	-	-
	[E.8] Difusión de software dañino	PP	M	B	B	-	-
	[E.9] Errores de [re-]encaminamiento	PP	-	-	B	-	-
	[E.10] Errores de secuencia	PP	-	B	-	-	-
	[E.15] Alteración accidental de la información	PP	-	M	-	-	-
	[E.18] Destrucción de información	PP	M	-	-	-	-
	[E.19] Fugas de información	PP	-	-	B	-	-
	[E.20] Vulnerabilidades de los programas (software)	PP	B	B	B	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	-	-	-
	[A.5] Suplantación de la identidad del usuario	PP	-	B	B	M	-
	[A.6] Abuso de privilegios de acceso	PP	B	M	B	-	-
	[A.7] Uso no previsto	P	M	M	M	-	-
	[A.8] Difusión de software dañino	PP	B	B	B	-	-
	[A.9] [Re-]encaminamiento de mensajes	PP	-	-	B	-	-

	[A.11] Acceso no autorizado	PP	-	M	M	-	-
	[A.15] Modificación deliberada de la información	PP	-	B	-	-	-
	[A.18] Destrucción de información	PP	M	-	-	-	-
	[A.19] Divulgación de información	PP	-	-	M	-	-
	[A.22] Manipulación de programas	PP	M	B	B	-	-
[sw4] Oracle 11g	[E.2] Errores del administrador	P	M	M	M	-	-
	[E.8] Difusión de software dañino	PP	B	B	B	-	-
	[E.18] Destrucción de información	P	A	-	-	-	-
	[E.19] Fugas de información	PP	-	-	M	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	M	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	-	-	-	-
	[A.7] Uso no previsto	PP	M	M	M	-	-
	[A.8] Difusión de software dañino	PP	B	B	B	-	-
	[A.19] Divulgación de información	PP	-	-	M	-	-
	[A.22] Manipulación de programas	PP	M	M	M	-	-
[sw5] Sistemas Operativos (Windows, Linux)	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[E.1] Errores de los usuarios	PP	M	M	M	-	-
	[E.8] Difusión de software dañino	PP	B	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	B	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	B	-	-	-
	[A.7] Uso no previsto	P	B	B	B	-	-
[sw6] Hipervisor (gestor de la máquina virtual)	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-

	[E.2] Errores del administrador	P	M	B	B	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	B	-	-	-
	[A.7] Uso no previsto	PP	M	B	M	-	-
	[A.11] Acceso no autorizado	PP	-	B	M	-	-
[sw7] Sistema de Gestión Documental RUMIDOCS	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[E.1] Errores de los usuarios	PP	M	M	M	-	-
	[E.2] Errores del administrador	P	M	M	M	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	M	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	-	-	-	-
	[A.5] Suplantación de la identidad del usuario	PP	-	M	M	M	-
[sw8] Respaldos (acronis)	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[E.2] Errores del administrador	P	M	B	B	-	-
	[E.15] Alteración accidental de la información	MR	-	M	-	-	-
	[E.18] Destrucción de información	P	A	-	-	-	-
	[E.19] Fugas de información	PP	-	-	M	-	-
	[E.20] Vulnerabilidades de los programas (software)	PP	M	B	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	M	-	-	-
	[A.18] Destrucción de información	P	A	-	-	-	-
	[A.19] Divulgación de información	PP	-	-	M	-	-
	[A.22] Manipulación de programas	PP	M	M	M	-	-

[sw9] Antivirus ESET	[E.2] Errores del administrador	PP	M	B	B	-	-
	[E.8] Difusión de software dañino	PP	B	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software)	P	M	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	P	M	M	-	-	-
[sw10] Monitoreo de Red PRTG	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[E.19] Fugas de información	PP	-	-	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	-	-	-	-
	[A.9] [Re-]encaminamiento de mensajes	PP	-	-	B	-	-
[sw11] Sophos SSL VPN Client	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[E.1] Errores de los usuarios	P	M	B	B	-	-
	[E.2] Errores del administrador	P	M	B	B	-	-
	[E.20] Vulnerabilidades de los programas (software)	PP	M	M	M	-	-
	[E.21] Errores de mantenimiento / actualización de programas (software)	PP	M	M	-	-	-
	[A.5] Suplantación de la identidad del usuario	PP	-	M	M	M	-
	[A.7] Uso no previsto	P	B	M	B	-	-
	[A.11] Acceso no autorizado	MR	-	B	M	-	-
[hw1]Servidores	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA	-	-	-	-

	[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[A.11] Acceso no autorizado	PP	-	A	A	-	-
	[A.23] Manipulación del hardware	PP	M	-	M	-	-
[hw2] Equipos Virtuales	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	P	M	B	B	-	-
	[E.23] Errores de mantenimiento / actualización de equipos	P	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	MA	A	-	-	-	-
	[A.11] Acceso no autorizado	MR	-	B	M	-	-
[hw3]Conmutador	[N.1] Fuego	P	M	-	-	-	-
	[N.2] Daños por agua	PP	M	-	-	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	P	M	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[A.11] Acceso no autorizado	MR	-	B	B	-	-
[hw4] punto de acceso inalámbricos	[N.1] Fuego	P	M	-	-	-	-
	[N.2] Daños por agua	PP	M	-	-	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-

	[I.7] Condiciones inadecuadas de temperatura o humedad	P	A	-	-	-	-
	[A.11] Acceso no autorizado	MR	-	B	B	-	-
[hw5] teléfonos ip	[N.1] Fuego	P	M	-	-	-	-
	[N.2] Daños por agua	PP	M	-	-	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.8] Fallo de servicios de comunicaciones	PP	M	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	P	-	-	M	-	-
	[E.15] Alteración de la información	P	-	A	-	-	-
	[E.19] Fugas de información	P	-	-	M	-	-
	[A.7] Uso no previsto	P	-	M	M	-	-
	[A.9] [Re-]encaminamiento de mensajes	P	-	-	M	-	-
	[A.14] Interceptación de información (escucha)	P	-	-	A	-	-
[hw6] informática personal (Computadores Todo en Uno, computador de escritorio, laptops)	[N.2] Daños por agua	PP	M	-	-	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.*] Desastres industriales	P	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	-	-	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M	-	-	-	-
	[E.24] Caída del sistema por agotamiento de recursos	P	M	-	-	-	-
	[A.6] Abuso de privilegios de acceso	PP	M	M	M	-	-
	[A.7] Uso no previsto	P	M	B	M	-	-
[hw7] Firewall	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*] Desastres naturales	P	A	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	A	-	-	-	-

	[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA	-	-	-	-
	[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M	-	-
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	A	-	-	-	-
	[A.11] Acceso no autorizado	PP	-	A	A	-	-
	[A.23] Manipulación del hardware	PP	M	-	M	-	-
[com1] red telefónica	[N.1] Fuego	P	M	-	-	-	-
	[N.2] Daños por agua	PP	M	-	-	-	-
	[N.*] Desastres naturales	PP	M	-	-	-	-
	[I.5] Avería de origen físico o lógico	P	M	-	-	-	-
	[I.8] Fallo de servicios de comunicaciones	PP	M	-	-	-	-
	[A.14] Interceptación de información (escucha)	P	-	-	A	-	-
[com2] red de datos	[I.8] Fallo de servicios de comunicaciones	PP	M	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	PP	-	-	M	-	-
	[E.10] Errores de secuencia	PP	-	M	-	-	-
	[A.9] [Re-]encaminamiento de mensajes	PP	-	-	M	-	-
	[A.11] Acceso no autorizado	PP	-	B	B	-	-
[com3] wifi	[I.8] Fallo de servicios de comunicaciones	P	M	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	P	-	-	B	-	-
[com4] red local	[I.8] Fallo de servicios de comunicaciones	PP	B	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	P	-	-	M	-	-
	[E.10] Errores de secuencia	P	-	M	-	-	-
	[A.5] Suplantación de la identidad del usuario	P	-	M	M	M	-
	[A.9] [Re-]encaminamiento de mensajes	P	-	-	M	-	-

	[A.11] Acceso no autorizado	PP	-	M	-	-	-
[com5] red virtual	[I.8] Fallo de servicios de comunicaciones	PP	M	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	P	-	-	M	-	-
	[E.10] Errores de secuencia	PP	-	M	-	-	-
	[A.9] [Re-]encaminamiento de mensajes	P	-	-	B	-	-
	[A.11] Acceso no autorizado	PP	-	M	-	-	-
[com6] VPN	[I.8] Fallo de servicios de comunicaciones	PP	B	-	-	-	-
	[E.9] Errores de [re-]encaminamiento	P	-	-	M	-	-
	[E.10] Errores de secuencia	P	-	M	-	-	-
	[A.5] Suplantación de la identidad del usuario	PP	-	M	M	M	-
	[A.11] Acceso no autorizado	PP	-	M	-	-	-
[SI1]discos	[E.15] Alteración de la información	PP	-	B	-	-	-
	[E.19] Fugas de información	P	-	-	M	-	-
	[A.15] Modificación de la información	PP	-	B	-	-	-
	[A.19] Revelación de información	PP	-	-	B	-	-
[SI2] memorias USB	[E.15] Alteración de la información	PP	-	B	-	-	-
	[E.19] Fugas de información	P	-	-	M	-	-
	[A.15] Modificación de la información	PP	-	B	-	-	-
	[A.19] Revelación de información	PP	-	-	B	-	-
[SI3] material impreso	[E.15] Alteración de la información	PP	-	B	-	-	-
	[E.19] Fugas de información	PP	-	-	M	-	-
	[A.15] Modificación de la información	PP	-	B	-	-	-
	[A.19] Revelación de información	PP	-	-	B	-	-
[aux1] Equipos de climatización	[I.3] Contaminación medioambiental	P	M	-	-	-	-

[aux2] Fuentes de alimentación	[I.3] Contaminación medioambiental	P	M	-	-	-	-
[aux3] cableado de datos (fibra y de alimentación)	[I.3] Contaminación medioambiental	PP	A	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	A	-	-	-	-
[aux4] sistema de alimentación interrumpida	[I.3] Contaminación medioambiental	PP	M	-	-	-	-
[aux5] sistema de video vigilancia	[I.3] Contaminación medioambiental	PP	M	-	-	-	-
	[I.7] Condiciones inadecuadas de temperatura o humedad	PP	M	-	-	-	-
[i1] edificio	[N.1] Fuego	P	A	-	-	-	-
	[N.2] Daños por agua	P	A	-	-	-	-
	[N.*.1] Tormentas	P	A	-	-	-	-
	[N.*.4] Terremotos	PP	M	-	-	-	-
	[I.*] Desastres Industriales	P	M	-	-	-	-
[p2]administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.	[E.4] Errores de configuración	P	-	A	-	-	-
	[E.19] Fuga de información	PP	-	-	A	-	-
	[E.28] Indisponibilidad del personal	PP	M	M	M	-	-
	[A.29] Extorsión	PP	M	A	A	-	-
[p1]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática	[E.4] Errores de configuración	P	-	A	-	-	-
	[E.19] Fuga de información	PP	-	-	A	-	-
	[E.28] Indisponibilidad del personal	PP	M	M	M	-	-
	[A.29] Extorsión	PP	M	A	A	-	-

Nota: Valoración de los activos realizado en PILAR.
Elaborado por: Autores

ANEXO F TRATAMIENTO DE RIESGOS

Tratamiento del riesgo en los activos considerados como críticos.

Tabla 24 Tratamiento del riesgo en los activos

ACTIVOS	AMENAZAS	Dimensión	Riesgo	Criticidad	Probabilidad	Estrategia
[is1] Voz sobre IP	[A.7] Uso no previsto	C	2,1	Medio	P	Mitigar
	[A.7] Uso no previsto	D	2,1	Medio	P	
	[A.7] Uso no previsto	I	2,1	Medio	P	
[is3] Servidor de Nombre de Dominio DNS	[A.11] Acceso no autorizado	C	2,3	Medio	PP	Mitigar
	[E.2] Errores del administrador del sistema / de la seguridad	I	2,3	Medio	PP	
	[A.11] Acceso no autorizado	I	2,3	Medio	PP	
	[E.2] Errores del administrador del sistema / de la seguridad	C	2,3	Medio	PP	
[ss1] Servicio de Impresión	[A.5] Suplantación de la identidad del usuario	I	2,7	Medio	P	Mitigar
	[A.7] Uso no previsto	D	2,1	Medio	P	
	[A.7] Uso no previsto	C	2,1	Medio	P	
	[A.7] Uso no previsto	I	2,1	Medio	P	
[ss2] Servicio de alojamiento	[A.18] Destrucción de información	D	2	Medio	PP	Mitigar
[sw1] Sistema Financiero CGWEB	[I.5] Avería de origen físico o lógico	D	2,1	Medio	PP	Mitigar
[sw4] Oracle 11g	[E.18] Destrucción de información	D	2,9	Medio	PP	Mitigar
[sw8] Respaldos (acronis)	[E.18] Destrucción de información	D	2,9	Medio	PP	Mitigar
	[A.18] Destrucción de información	D	2,9	Medio	PP	
	[I.5] Avería de origen físico o lógico	D	2,1	Medio	PP	
[sw9] Antivirus ESET	[I.5] Avería de origen físico o lógico	D	2,1	Medio	PP	Mitigar
[sw11] Sophos SSL VPN Client	[I.5] Avería de origen físico o lógico	D	2,1	Medio	PP	Mitigar
[hw1]Servidores	[I.7] Condiciones inadecuadas de temperatura o humedad	D	2,6	Medio	PP	Mitigar
	[N.2] Daños por agua	D	2,3	Medio	PP	Asumir
	[I.5] Avería de origen físico o lógico	D	2,3	Medio	PP	Mitigar
	[N.1] Fuego	D	2,3	Medio	PP	Asumir
[hw2] Equipos Virtuales	[E.24] Caída del sistema por agotamiento de recursos	D	3,5	Alto	P	Mitigar
	[N.2] Daños por agua	D	2,3	Medio	PP	Asumir
	[I.5] Avería de origen físico o lógico	D	2,3	Medio	PP	Mitigar
	[N.1] Fuego	D	2,3	Medio	P	Asumir
[hw4] punto de acceso inalámbricos	[I.7] Condiciones inadecuadas de temperatura o humedad	D	2,1	Medio	PP	Mitigar
[hw5] teléfonos ip	[E.15] Alteración de la información	I	2,6	Medio	PP	Mitigar
	[A.14] Interceptación de información (escucha)	C	2,1	Medio	PP	Mitigar
[com1] red telefónica	[A.14] Interceptación de información (escucha)	C	3,1	Alto	PP	Mitigar
[com3] wifi	[I.8] Fallo de servicios de comunicaciones	D	2,6	Medio	PP	Mitigar
[i1] edificio	[N.1] Fuego	D	3,0	Alto	PP	Asumir
	[N.2] Daños por agua	D	3,0	Alto	PP	Asumir
	[N.*.1] Tormentas	D	3,0	Alto	PP	Asumir
[p2]administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.	[E.4] Errores de configuración	I	2,1	Medio	PP	Mitigar
[p1]administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática	[E.4] Errores de configuración	I	2,1	Medio	PP	Mitigar
[hw7]Firewall	[I.7] Condiciones inadecuadas de temperatura o humedad	D	2,6	Medio	PP	Mitigar
	[N] Desastres Naturales	D	2,3	Medio	PP	Asumir
	[N.1] Fuego	D	2,3	Medio	PP	Asumir
	[N.2] Daños por agua	D	2,3	Medio	PP	Asumir
	[I.5] Avería de origen físico o lógico	D	2,3	Medio	PP	Asumir
	[E.23] Errores de mantenimiento / actualizaciones	D	2,2	Medio	PP	Asumir

ANEXO G VALORACIÓN DE ACTIVOS

Información de la valoración de activos realizado por el Jefe de Tecnología en conjunto con autores.

RECOLECCIÓN DE INFORMACIÓN	
NOMBRE:	LUIS VILLALTA
TÍTULO:	INGENIERO EN SISTEMAS
CARGO QUE OCUPA:	JEFE DE TIC´S
ACTIVIDAD:	VALORACIÓN DE ACTIVOS INFORMÁTICOS
DIMENSIONES DE CALIFICACIÓN	
[D]	DISPONIBILIDAD
[I]	INTEGRIDAD
[C]	CONFIDENCIALIDAD
[A]	AUTENTICIDAD
[T]	TRAZABILIDAD
DIMENSIÓN	**PREGUNTA**
Confidencialidad	¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
Integridad	¿Qué importancia tendría que los datos fueran modificados fuera de control?
Disponibilidad	¿Qué importancia tendría que el activo no estuviera disponible?
Autenticidad	¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
Trazabilidad	¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?
	¿Qué importancia tendría que no quedara constancia del acceso a los datos?
CRITERIO DE VALORACIÓN	
Nivel	**Criterio**
10	Nivel 10
9	Nivel 9
8	Nivel 8(+)
7	Alto
6	Alto (-)
5	Medio (+)
4	Medio
3	Medio (-)
2	Bajo (+)
1	Bajo
0	Depreciable

	[D]	[I]	[C]	[A]	[T]
[B] ACTIVOS ESENCIALES					
[E1] Información Confidencial		9	9	9	8
[IS] SERVICIOS INTERNOS					
[is1] Voz sobre IP	8			8	8
[is2] Internet	7			8	7
[is3] Soporte al usuario	7			3	7
[is4] Servidor de nombres de dominio	7			7	7
[SS] SERVICIOS SUBCONTRATADOS					
[ss1] Impresión	7			3	5
[ss2] Alojamiento de servidor Web	7			6	6
[ss3] Correo Electrónico	7			7	7
[ss4] Proveedor de servicio de internet	8			8	8
[ss5] Respaldo de datos	7			8	6
[ss6] Alojamiento de aplicaciones (hosting)	7			7	7
[SW] APLICACIONES					
[sw1] Sistema Financiero CGWEB		9	9	9	9
[sw2] Ofimática					7
[sw3] Servidor de directorio		9	9	9	9
[sw4] Sistema de gestión de base de datos (Oracle 11g)					7
[sw5] Sistema operativo (windows, linux)					7
[sw6] Hipervisor (gestor de la máquina virtual)					5
[sw7] Sistema de Gestión Documental RUMIDOCS		8	8	8	8
[sw8] Respaldos (acronis)					7
[sw19]Antivirus (ESET)					7
[sw10] Monitoreo de Red (PRTG)					7
[sw11] Sophos SSL VPN Client					7
[HW] EQUIPAMIENTO INFORMÁTICO					
[hw1]Servidores	9	9	9	9	9
[hw2] Equipos Virtuales	9	9	9	9	9
[hw3]Conmutador					8
[hw4] Punto de acceso inalambricos					8
[hw5] Teléfonos ip					6
[hw6] Informática personal (Computadores Todo en Uno, computador de escritorio, laptops)					8
[hw7] Firewall	9	9	9	9	9
[COM] REDES DE COMUNICACIONES					
[com1] Red telefonica		7			
[com2] Red de datos					7
[com3] Wifi					7
[com4] Red local					7
[com5] Red virtual					7
[com6] VPN				8	8
[SI] SOPORTES DE INFORMACIÓN					
[SI1] Discos		7	7		
[SI2] Memorias USB		7	7		
[SI3] Material impreso		7	7		
[AUX] EQUIPAMIENTO AUXILIAR					
[aux1] Equipos de climatización	7				
[aux2] Fuentes de alimentación	7				
[aux3] Cableado de datos (fibra y de alimentación)	7				
[aux4] Sistema de alimentación interrumpida	7				
[aux5] Sistema de video vigilancia	7				
[L] INSTALACIONES					
[i1] Edificio			8		
[P] PERSONAL					
[p2] Administradores de sistemas Ing. Luis Villalta - Jefe de TIC´s.			8		
[p1] Administradores de comunicaciones Sr. Ismael Aldaz – Técnico en Informática			8		

Ing. Luis Villalta

JEFE DE TIC´s